#125 - Cyber Ranges (with Debbie Gordon)

[00:00:00]

[00:00:12] **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, and I'm your host today. And what we want to talk about is policy, practice, and proof, and I have a special guest today, Debbie Gordon.

But before I get started, just a quick reminder, if you're not already watching us on YouTube, please do so. We've got a YouTube channel. Follow us. Subscribe. You get to see my shiny happy face. Plus, get the information in a format that a lot of people like to consume. Helps us get the word out to others.

And if you're listening to us in the podcast, again, subscribe. If you're not already doing so or let other people know. Follow us on LinkedIn because we've got a lot more than just podcasts. So there's a quick preamble to our show here with Debbie. Let me talk a little bit about our [00:01:00] background on this subject.

So on episode #116, we had Michael Krausz come on and talk about ISO and the CISO responsibilities. And one of the key pieces of information that he had mentioned is there are three dimensions to an effective information security management system. Call those the three Ps: Policy, Practice, and Proof.

Well, on today's episode, we're going to dive into these concepts even more to talk about how organizations can leverage the three Ps to build something that's truly polished. Let's start with policy and we'll find that many organizations' cybersecurity policies are based on ISO 27001, or NIST CyberSecurity Framework or some other type of structured external document like that.

And in a proper cybersecurity policy, we're going to reference information security controls or outcome driven statements. Let's take an example. In ISO 27001, control 5.26 says information security incidents shall be responded to in accordance with the [00:02:00] documented procedures and control. 5.27 states knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.

Okay, these are two good objectives to have in a policy. They're fairly high level, but they define outcomes that organizations want to achieve. Now, once we have a policy in place, We need to ensure that the organization's practices what's on paper. Remember, when the proverbial stuff hits the fan, we're going to fall back to our level of practice.

So let's take the example of archery. We have archery safety rules. That is a policy that will likely include the following rules among others. Only point the bow in a safe direction. Never point the bow at a person, even if no arrow is knocked. Be aware of what is in front of and behind you. Now, following these three safety policies doesn't make you an accurate shooter.

You need to practice shooting at the range. But if you practice at an archery range, and you'll [00:03:00] experience important concepts like bow control, arm fatigue, breathing, proper stance, line of sight, and proper release, and this shooting practice at an archery range creates an opportunity to document mistakes when we miss the bullseye and when this occurs, we should ask ourselves or professional coach. Two questions. Number one, why did I miss the target? And number two, what can I do differently? Going forward now, asking these two questions allows us to learn and to get smarter in our next practice session at the range. Our third P is proof. And at the end of the day, any compliance standard needs evidence or proof to show that an organization is performing to its desired objective.

And these are the things that the audit team wants to see. So if we have a policy that says incidents shall be responded to according to our documented procedures. That we need to show that during our last cyber event, we followed those procedures. For example, your incident [00:04:00] response plan may say you need to notify John Smith, who's the incident response commander.

And if the incident escalates, then we have to notify the CIO, Julie Williams. So be sure you log the time you brought John and Julie into the discussion. And this record establishes evidence that your procedures were followed, and this evidence chain shows that you are following the procedures and ultimately displaying the proof that you have an effective cybersecurity program.

Well, now I'm excited to bring on her special guest who's been very patiently listening to me while doing my little monologue. Debbie Gordon from Cloud Range Cyber will talk about how she is applying the concepts of ranges to help organizations. And Debbie, welcome to the show.

[00:04:40] **Debbie Gordon:** Thank you G Mark.

[00:04:42] **G Mark Hardy:** Now, can you tell us a little about yourself and your background?

[00:04:45] **Debbie Gordon:** Sure. So my background started quite a long time ago, but relevant background about almost 30 years ago. I started my career in the technical education space. And back then in the mid nineties, when the [00:05:00] CNE and MSCE and CCNA certifications were a thing they were really important for people who wanted to get into those types of careers because when somebody had those certifications, they were able to get a job and they were able to do a job.

But fast forward all these years cyber is a whole different story and what I realized, Over time and building, building several companies in the meantime was that the cyber talent shortage isn't just about empty seats in cybersecurity. It's about the fact that the people who are already employed in seats in cybersecurity are only as good as their experience.

And so in order for us to really close that skills gap, We have to close the experience gap and the experience gap is just about giving people more experience without doing it in a production environment. So when I founded Cloud Range it was for the sole purpose of accelerating [00:06:00] experience to reduce risk in organizations and working with cyber defense teams.

[00:06:05] **G Mark Hardy:** Now that makes sense. And you said you've started a number of businesses, but now you're in the range business. And what, why, what makes that so special? Why this is sounds important and I think it really is,

[00:06:15] **Debbie Gordon:** There are a lot of training products and training companies and training methods in cybersecurity, and you're probably familiar with many of them. There's, you know, there's, there's three types of learning. Knowledge is one, skills are another, and then abilities is another. And so, Knowledge is something, there's plenty of knowledge out there.

You can read books on cybersecurity. You can watch videos, you can listen to your podcasts. You can get skills. You know, you can learn how to, how to write firewall rules. You can learn how to do very specific individual linear skills in cybersecurity. But what was missing? Was experience true experiential learning, and that's what we do on a range.

And so I, I just saw a huge opportunity in the world to fulfill [00:07:00] that last mile because lots of people have acknowledged, lots of people have skills. But the abilities, how do you actually know when to use those skills, how to use

them and why to use them in a highly pressurized environment. So think of it like it's a flight simulator if you're not practicing on a flight simulator.

You may know how to adjust the temperature. You may know how to, how to put the landing gear down. You may know how to do individual things, but if you're flying a plane knowing exactly what to do and how to do it when you're struck by lightning is a totally different game. And so that's why a range enables individuals and more importantly teams to be able to proactively prepare and practice and have proof back to your original topic of what they're doing and how effective this is.

[00:07:48] **G Mark Hardy:** And I think that proof is important because we're talking about the three Ps, the Policy, the Practice, and the Proof. But sometimes what happens is a lot of times we spend our efforts in, in creating our protect. Okay. We identify, [00:08:00] protect, detect, respond, recover. Oh, we're going to protect against everything.

We're never going to have a problem. Nothing's going to get in. But the reality is that stuff always gets in. And so then the real effort is going to be the respond and recover functions. But do you find organization sometimes kind of front load, they're posturing, figuring, well, we're just going to be awesome and no one's going to get through, and therefore they potentially neglect what you do when something does get through.

[00:08:24] **Debbie Gordon:** That's evolving. I would say five years ago even, I would say a lot more security leaders were very technology focused. So if you think about people, process, and technology, A lot more people back then, you know, in the dark ages five years ago, thought that technology could solve all problems. And then there's other people who layer on the compliance processes.

Well, if you do that, then we're good. But what people are now thankfully realizing is that the people are really the last line of defense. And they're the ones who have to be trained and [00:09:00] continuously trained to make sure that all of the policies, processes, and technology that are in place are practiced and validated.

[00:09:11] **G Mark Hardy:** And your people can really become your first and last lines of defense because, and that's educating your user base where they go, “that just doesn't look right.” Or, “I probably should be cautious about that.” And that's sort of how we know when we win when we've got non-technical executives who are spotting stuff and going, “that doesn't look right.”

They don't have to solve it, but need to bring us to our attention because one of the things that often takes place as a result of phishing or people clicking on things or picking up the random USB drive or the drive by all the other stuff. Let's take ransomware for an example. Okay? It can really affect an organization in a pretty serious way, and we've talked about earlier the importance of following procedures. And we can use incident drills as a way to strengthen our security controls, because, as you said, just like flying an aircraft I, I'm a private pilot, but I've never been struck by lightning, [00:10:00] and have I practiced that? No. But I have practiced a lot of other things.

Like I had a flight instructor always like at some point pulled the power back and said, all right. You have no engine, what are you going to do? And after a while, you don't wait till that takes place. You're constantly keeping in mind, okay, there's a field over there. Oh, there's an open area there, and you're in your mind, you're kind of leaping along.

So if you ever did lose the engine, you're good to go. But here, as we take a look at being able to respond to something like ransomware, how could you practice these sorts of things but not do it in the production environment? That sounds like a perfect case for having a range.

[00:10:35] **Debbie Gordon:** Yeah. And that, it is a great example. We do so many ransomware simulations, and there's, so there's two types of simulations you're probably familiar with the tabletop exercise. That's the one that, you know, many companies will do a few times a year. They'll get a bunch of people in a room and they'll, you know, a lot of them are not technical.

It might be a lot of people from the executive team, and in those, in those tabletop exercises, Something already happened. [00:11:00] So let's say the FBI comes in, they pretend the FBI comes in and they just said, oh my gosh, we just found a hundred thousand of your customers' records on the dark web. What do you do?

And then so it goes, you know, who does what, who doesn't do what? What are you supposed to say? What are you not supposed to say? What kind of decisions do you have to make to the media, to the, you know, what kind of technology decisions do you have to make? All of these things. But in those examples, in a tabletop exercise, something already happened.

So that's that. But what we do with, with ransomware, with cloud range, we're able to simulate a ransomware attack actually happening. So from the time that somebody sees something on their screen, To the time it is recovered on the

technical side. And I'll tell you, a ransomware attack in a simulation on the technical side is not an easy one.

So we actually never start customers with those when they're doing simulations every month. Ransomware is actually a more intermediate or advanced one. So we have a, a path to ransomware to get to that, but it's more, it's more about how do you make sure that you [00:12:00] minimize the damage and that you know what decisions you have to make on the technical side, so it doesn't get to the point of having to involve executives for some of the decisions that have to be made.

[00:12:12] **G Mark Hardy:** And one of the things that I think comes out of this is when you think about a range, A range is not one individual going in there, sitting in a classroom, going through a can set of exercises, and you get to do the exact same. You know, drill that every other student did last month and this month and next month.

This is team training and you can actually bring in your team together and work together on it because the interpersonal dynamics, I think are going to be a huge element of success or failure. So can you tell me a little bit of the benefits of being able to do team training and particularly how it pertains to ranges?

[00:12:46] **Debbie Gordon:** Yeah, absolutely. And that, and that is the most important part. It's, that's, as a team, you're able to exercise the skills, so you have a lot of skills. But. You're working with other people, you have to figure out what to [00:13:00] do and what your role is and what other people's roles are. The individual part, individual training is, is very important.

But that's like, you know, playing, playing baseball and knowing how to, how to field balls. You might be great at that. Or hitting a, you know, hitting a ball with a bat. But can you actually play the game? Two very, very different things. And so, the range, I, I want to touch on something you said to you, mark, is that, a cyber range can have many different meanings.

People think about them in different ways. Some, some of you may have been to a cyber range where you go and do a fun incident response exercise and you walk out of there thinking, oh my gosh, there's a lot more to a ransomware attack than I thought. Or some may think of a cyber range as you know, an individual going and doing a lab exercise with a few virtual machines.

That's kind of a step-by-step tutorial that can also be defined as a range the way we define our range is a full replica of an enterprise network with real tools. So

whatever, you know, SIEMs and firewalls and EDR solutions companies using [00:14:00] those, they get versions of those in that, in this environment there's real traffic, there's real malware, it's all contained.

So, Nothing gets onto a customer's network and they are able to go in and practice detecting and responding to attacks that we develop. So we script attacks, they run through, they are, they are propagating that range and that environment. And just like a SOC analyst has to do in their day-to-day job, they are looking at alerts, they're looking at traffic, and they don't know what they're looking for.

So if you've ever been to an escape room, You don't know what you walk in. You don't know what you're looking for. Somebody doesn't tell you to go look on that wall for a clue. You're just standing there. You don't even know where to start. And that's the same thing because that's how it happens in real life.

The attackers don't call you and say, Hey, by the way, I'm about to, you know, send an email from this IP address. You might want to go look at it. And so the range is an incredible way for people to safely hone their skills, not just as individuals, but as a team. Because as soon as you introduce other people, So when you're [00:15:00] doing something yourself pretty cut and dry, like think about landing gear, you know, or anything that a, a pilot is doing, a pilot's working on their own, they're making decisions.

But if you have a team, every move that one person makes is going to affect what the other people have to do or not have to do. And they have to be able to communicate and collaborate. And so it is. Imperative in cyber defense teams that ranges are used. Because you cannot depend on things to happen in real life, and be confident that people are going to know exactly what to do and when to do it and how to do it.

[00:15:33] **G Mark Hardy:** And there's something you'd mentioned that struck me as being very important. And the fact is, you create bespoke range events. It's not like you walk in and everybody gets the same thing. It's not like you're going to the arcade with a quarter and you get to play the same game you did yesterday, the day before, and everybody else in line for it.

You're able to tune that if I heard you correctly, to the client environment. So when you come in there, it's like, whoa. This is Unix. I know Unix, right? You [00:16:00] recognize the environment that you're working in, and that to me seems a lot more realistic than anything that would be artificial, that could have been created for mass production.

[00:16:08] **Debbie Gordon:** Right and you want to have muscle memory.

So again, just like flying an airplane, you want to already know what to do when it's happening. You don't want to have to think. So the more, the more you practice, the more muscle memory you have. The environments are the ranges that our customers use, they are intentionally very complex. They're real that it's not a video game. This is an actual real virtualized network. So with all very familiar things it doesn't necessarily need to be the exact same configuration cause we're at pen testing it, we're actually making it intentionally vulnerable so that the attacks that we build.

Can get through. But the defenders, the SOC analysts and, and the incident responders they have to be able to be critical thinkers. They have to be able to work together, they have to be able to communicate. And they take these attacks and they're, they're going all the way through recovery on these attacks.

And they're, they're [00:17:00] scored in a multitude of ways.

[00:17:02] **G Mark Hardy:** That's great. I remember a study that was done a few years ago, and it was aviation safety since we keep coming back to aviation and they looked at flight crews and typically you have a pilot in command who's large and in charge and makes all the decisions. And what they did is they created a number of simulated emergencies.

And what happened was that the pilots who said, I know what to do, and did it compared to those who stopped a moment and asked the co-pilot or the flight engineer, if you had one, what do you think we should do? The teams routinely did better than the single pilot because no one person could know it all.

And, as a result, all of us are better than one of us, and we have to remember that. And by being able to practice that in the range environment, you're emphasizing that, but also you're realizing the benefits, you're not sending somebody off for a one week training course. You spend a ton of money and you come back and look, I got a piece of paper and a whole bunch of books, and then where are those books?

One month, two months, six months later, Hey, hey, look at my books. I've got them on my shelf. As compared to, [00:18:00] wow, we went through this together. And I think that's huge. Now when you do that, organizations that practice together, end up doing better. Their processes are better, they're a little bit cleaner, their handoffs work better.

And if we think about it when we're kids, I mean, schools used to do fire drills and the teachers and students who know how to safely leave a building in a timely manner, and you do that on a regular basis. You could keep track of it and the principal's sitting with the stopwatch and timing it and you get better and everybody gets out there, they get to the right places, fewer people get confused and things such as that.

Well, with that speed improvement, you know that you could probably save some lives in the event of a real fire in a school. Have you seen speed advantages or things getting faster in cyber?

[00:18:44] **Debbie Gordon:** Absolutely. That's why we do what we do. At the end of the day, it's about speed. I mean, on the, on the data security side it's about speed and minimization of, of data exfiltration on the OT side. You know, it's about uptime, so yeah, very some, sometimes they're [00:19:00] conflicting if, if teams aren't aligned. But that's a whole, that's for another podcast.

But yeah, the detection and response time. So, you know, if you think of mean time to detect and mean time to respond. Those are, those are lagging indicators. Those are usually what happened in a period of time, a month or a quarter or a week in the past, in the real production environment. But by doing simulated attacks on our cloud range, cyber range, we can look at benchmarks on time to detect, not mean time to detect, actual time to detect a certain attack.

And time to respond and compare that against benchmarks in our industry and among our user base. And show improvements over time in, in how even on a very different type of attack how teams perform and watch that improve. And that's a leap that becomes a leading indicator. So if they're doing it proactively, we can say that well they've now, they have done [00:20:00] better than the average of the detection time on a certain type of attack. And that's a leading indicator that's saying that, you know, they're, they're improving over time. And that's, you know, that's what boards want. They want to see improvement. They know that nobody's perfect.

But as long as organizations are improving and they're being proactive in doing that, they're going to keep it, making these types of investments.

[00:20:22] **G Mark Hardy:** And you'd mentioned boards and I, I think what we find then is that as a technical level, we often deal with measures. Okay, here's the data. Okay. How'd you do? Did a 93. Okay. Well, How well did you do the last time? Well, I made 110 times or own to 93 is compared to, well I finally got up there. So then we go to metrics, which are some information trend over time.

But then we get to KPIs. So key performance indicators, which are really going to be your metrics over time with basically target goals and things to say, I want to get here and I, maybe I'm not there, or I have reached that. That's the best way to communicate that information to executives and to justify, not only has your investment in your [00:21:00] cybersecurity team been worth it, Is our ongoing training and practice producing measurable results that allow us to say, not only have we gotten better, but we meet or exceed what would be benchmark goals out there?

How powerful is that in terms of being able to drive a business case, particularly if we're looking at some potential slowdown in financial spending over the next 12 months to go back and say, these are dollars that you really, really, need to spend. They're some of the most valuable ones you get.

[00:21:26] **Debbie Gordon:** Well, they are, first of all, people are the most valuable asset in a security stack. They're the ones that, you know, companies make investments in and they have the opportunity to maximize their value. You know, think of shelfware. A lot of software is purchased, is not necessarily tuned properly or maximized.

The use of people have to be treated the same way obviously as people. But they're giving them the opportunity to train and become the best that they can be for the sake of reducing risk in the organization should be a huge priority. So when we look at. Quantifying [00:22:00] that. So there, there's a couple of areas that we, or I'll, I'll say categories that we show that growth in.

So number one is competencies. So, There are different frameworks of of competencies for different roles. So if you're familiar, probably many of you're familiar with the NICE framework. So, in the NICE framework there are over 50 work roles. And in each of those work roles they, you know, think about like a job description.

But in that, in that description, there are knowledge and competency statements. So if you're a n entry level SOC analyst, you need these 91 competencies. And you know, a person may only have 60 of those, well, the remaining 31, that represents risk. If the company agrees that they need 91 and they only have 60, that's a gap.

That's a, that is a human vulnerability right there. And so we're able to show that gap going closer. You know, the, the closing the gap of instead of 60, now they have 80. Now they have 90, and now they have [00:23:00] 91, and now they

even. Another 50 additional ones that will prepare them for their next role in the company.

So that's competencies. So, the cyber professionals in the organization are, are measured and it's not for the sake of saying, Hey, you know what G Mark, you're not really competent. It's to show where the areas for improvement are to enable people to go, you know, get budget approved for it, to show visually that there I and objectively that there is a gap there. Now the second area is the content. So there's competencies, what somebody is able to do, but then when we look at different attacks we use the Mitre ATT&CK® Framework to develop attacks. And as you know, there's an infinite number of TTPs.

You know, we can, we can develop attacks all day long. But when we use the Mitre ATT&CK® Framework, we're able to visually show which different parts of that matrix have been accomplished successfully by that team and more importantly, what's left [00:24:00] and what has to be done to accomplish those. So some types of things may be more applicable to certain industries.

And so they may want to prioritize doing those and, and they may want to, you know, not spend as much time on something that they may not really be as vulnerable to. But it is a way to provide a framework that is understandable, and especially for boards and c-suites, they don't need to know the details of the types of attacks in a, in the Mitre ATT&CK® Framework

they just need to see what's being done, and again, more importantly, what continues to be done to close that gap.

[00:24:33] **G Mark Hardy:** somehow I, I think putting up that whole tactics and techniques or Mitre ATT&CK® Framework is not the board level slide you want as a CISO to go ahead and just hit him with that eye chart. But as you mentioned that though, If we combine the concept of using the Mitre ATT&CK® Framework with our threat intelligence, what allows us to do is then craft scenarios that are more likely to occur than others that are going to represent the, the biggest threat, [00:25:00] which again, we go back and say, well, why should we do this?

Or, why is this a generic scenario? And you go back to the, the, your boss or your board or whatever, say, no ma'am, this is not a generic scenario. This is actually deliberately chosen based upon what we perceive to be our threats. We've looked at the tool sets that we have here, and now we structure this environment so we can demonstrate over time, measurable progress toward a goal.

[00:25:22] **Debbie Gordon:** Right. and those, and the attacks can be proactively developed using the framework, but we're also responding to if, if a customer says, Hey, you know, a competitor just got this, just got hit with, you know, X, Y, Z. Can you create this? We will create it if we don't already have it or some version of it.

And then third is we're looking at CISA advisories and we're, we're creating attacks based on things that, that are coming through the advisories as well. So very proactive in that way.

[00:25:54] **G Mark Hardy:** And I think the advantage of being able to run your team through scenarios like this is you can get a little bit faster [00:26:00] and you get a little bit more efficient. So for me, as a retired naval officer, I got to tell you, one of the most, you know, frightening things on a ship is to have a fire. And it's like, well wait.

You're surrounded by fire. You just put water on the fire and the fire goes out. Right? But then you sink. And so you have a, time is running and time is absolutely of the essence when you're doing damage control, but it's important that you don't do the wrong things or you could end up, you know, jeopardizing the ship or losing all hands and things like that.

Most of the time we're not facing life and death situations in the cyber, but we do have incident response playbooks. We pull these things out and we should be running those through the events. And sometimes in the scenarios we come up with situations that we haven't identified or we don't know whom to notify or who's the decision maker here?

Well, we didn't think of that when we wrote our playbook, but now we have a scenario that's been presented, which means somebody's taken notes saying We need to go back to the drawing board on that. Have you found common gaps in either policies or procedures that your teams have uncovered when you're looking at [00:27:00] folks going through and running through the cyber range.

[00:27:02] **Debbie Gordon:** I think it's more of a general general statement to answer that is that until people practice what's on paper does not matter. It really doesn't matter. It looks good on paper, but until you, until you're doing it, there's so many variables that could happen. I mean, even if you just as a team not knowing well, who, like you said, well, we don't, this is new.

Who's supposed to do that? And then all of a sudden you're scrambling and then everything halts. So, it, it just goes back to the fact that what's on paper even the

process on paper may or may not be good. But until you practice it, you have no idea if it's even doable

[00:27:41] **G Mark Hardy:** yeah, and it, so let me ask a little query similar to that. So one of the things that came up with my, my talk with Michael that we did a few months ago, Michael's from Austria, and he had said something that kind of caught me off guard. He said, when you Americans write things, it's very, very Uh, specific, you shall do this, do this, do this.

You basically spell everything out [00:28:00] in detail, so they're telling you how to drive. And over here in Europe at the iso, we basically say, here's your goal. Get there, use your brain. And, and of course the old saying from Old World War II was from the German officers said the hard part about fighting the Americans, they don't even follow their own doctrine.

And so therefore you never know what they're going to do. And of course, from Michael's perspective was the complete opposite. Have you seen in the teams that go through there any, I dunno if it could be cultural differences or or performance differences, and is there been advantage of one over the other?

And maybe if it's not by nation, it might be by how they train? Do they train toward like an ISO standard or a cybersecurity

framework? Is there anything there that you can observe?

[00:28:40] **Debbie Gordon:** We've seen cultural differences and not necessarily to how this, you know, following standards, but we've seen very distinct and very interesting. Cultural differences. And I'll give you a a real example. We have a customer who has a follow the sun model with their [00:29:00] SOC and they have one team in the US and one team in another country. I'm not going to say which one. So I might give it away. For all intents and purposes are the same, same skills, same roles. It's not, you know, it's not tier one or tier or two or level one, level two. Anyway, so for all intents and purposes, same thing. Just follow the sun. So we do simulations with each team, but separately. So on a Monday we may do the US team, and on a Tuesday we may do the overseas team.

The overseas team, culturally, Does not talk very much. And they're doing the same exercise as the US team. The US team always outperforms and they're not competing against each other. It just happens to be doing, you know, one day. And then the other day the US team outperforms the other team on detection and response and collaboration significantly because and, and.This is there's a

lot [00:30:00] to this. In some cultures people will not do something or ask a question unless they're you know, sometimes people don't ask questions because it's not culturally acceptable. But in incident response, teamwork and seeing what you, or saying what you see, if you see something, say something.

It is so integral. Because a lot of times people will, you know, in a forensics exercise, they might find an artifact and we can see their screens. So we know if they found something, but it might be an hour before they say anything because they weren't a hundred percent sure and they wanted somebody else to find it first and think about the cost of that hour.

[00:30:37] **G Mark Hardy:** Wow.

[00:30:37] **Debbie Gordon:** And so, yeah, so there there's very distinct differences and that also has to do with leadership. So SOC managers. Are the, the way that they encourage people to especially in our, in our trainings, we encourage people to talk. We encourage people to see what they saying, even if they're not sure.

No, and we always tell people, nobody's getting fired for making a mistake in a, in a simulation, we want [00:31:00] people to make mistakes. We want people to push the boundaries. We don't want them to go rogue. And we've seen that happen too. And somebody, you know, shuts down a website and doesn't mention it to anybody, and then all of a sudden the exercise is dead.

But leadership is so important. So, you know, anyone who's thinking, you know, as, as they move up the ranks in security leadership most of you probably didn't sign up to, you know, work on soft skills with your teams. But that is honestly the weakest link in the chain in cyber defense because people can have great technical skills, but if they're not working together and collaborating, it has a drastic negative impact on the result.

[00:31:35] **G Mark Hardy:** And that of course makes perfect sense as you say that. So I'm glad you didn't mention the company, because then the attackers should know, okay, go after them on, you know, when it's nighttime over here in North America. So, so that worked out well. But for an, a team that let's say has a series of procedures and maybe they're not following them effectively, the, the management's concern that, hey, it's malware and they're trying to identify the [00:32:00] malware and they're figure it out instead of containing it first.

And they, they, they got their PICERL out of order and they're instead of like containing, they're then trying to try to eradicate and then it just keeps spreading

and things like that. Or they forgot to make a forensic copy, they just want to get rid of it. And there's nothing for law enforcement. Now sometimes we have regulatory requirements, we have compliance requirements that say you're supposed to do things in the right order and do them.

And it sounds like if I go to a range and say I'm a bit concerned as a team leader here that my people might be missing things. Can we structure an exercise that is going to position these do A before B, before C, effectively? So that is this part of this bespoke exercise. I'm actually looking for the things that I've already realized that my team needs to improve on.

[00:32:47] **Debbie Gordon:** Absolutely. So during, during the cloud range exercises, we can utilize a customer's playbook and so all the, the processes and procedures that are required in their organization. We can [00:33:00] use those and they can be tested on them. And what happens is that they end up getting adapted because they realize once they go through them, they say, oh, wait, this isn't quite right.

Right? I think we need to change this a little bit, but we're able to measure the alignment of it first, and then we're able to say, well, even though they aligned with it, is this the actual, is this the, in fact, the best way to do it.

[00:33:21] **G Mark Hardy:** Mm-hmm. And as we get our people and the teams in there, part of what we can do, it seems, is workforce development. So in large organizations we have well defined roles, and someone starts out as a junior cyber analyst. Really wants to have some sort of a career objective to go forward. Maybe you want to be a senior analyst or whatever the next level happens to be, your a target, but they have to demonstrate some levels of the the knowledge and skills and abilities if you will.

The, you know, the ksa. What are things that you range could do to help a manager in terms of positioning their workforce development efforts to say, I can get people there and they can come back. And now not only have I got measurable, [00:34:00] Capabilities, but I could possibly put them in the next higher role to see how well they do and if they crash and burn, no worry. It's a simulation. You start all over again. But have you seen that, that we could use as a range for workforce development?

[00:34:12] **Debbie Gordon:** Just in general with workforce development. You know, we, we think of workforce development in two ways. One is creating new workforce outside of a company that aren't employed yet. And then the other one is workforce development within a company and developing employees,

whether they're already in cyber or maybe they're in marketing and they want to get in cyber.

But you know, how, how do you take somebody who's already employed and grow their career within the company? Because remember, retention is just as important as hiring cause retention. It's really hard with the, with the shortage. So we are able so you mentioned the, the KSAs, the knowledge, skills, and abilities.

So we're able to obviously track and do an inventory, if you will, of what individuals competencies are. And then it may show that, oh, you know what? You have all these extra competencies, but you are already qualified to go do this job.[00:35:00] But first and foremost there's, there's two assessments that we, that we have, that our customers use.

And they're really, one of the first one is just, is the coolest thing because it's it's an, it's a cognitive aptitude assessment and In short, it's, your brain was born to be good at X, Y, or Z but maybe not A, B or C. And so everyone thinks, you know, if you ask a teenager, Hey, what does it mean to get in to be in cybersecurity?

They're good. They'd say, oh, you know, a hacker. Because that's all they know from tv. But the, you know, the fact of the matter is there's over 50 different roles in cyber, and those roles use different parts of the A SOC analyst or a forensics analyst uses very different parts of the brain than a pen tester.

And so the the, it's called right track, the right track cognitive aptitude assessment that we have is. It's a, it's a, I'll call it brain tests. Having nothing to do with cyber, but the output of it says, okay, G Mark, you would be [00:36:00] great in defensive operations because of the way you think and, and here's why.

And then it would have a prescription of, here's all the training you need to do and the KSAs to be in a job. So that's something great that companies are using both for their existing cyber talent and also people that they're bringing in from the outside. And people that they may be bringing in from other departments to get into cyber because somebody in marketing may be really great at something in cyber, but they may think that they don't have a technical background.

But as we all know, or hopefully all of us know now, is that you don't need a technical background to get into cyber. The second thing is we have actual range immersion assessments where if somebody is interviewing for a job either

from the outsider or from within. They may have a great resume, they may have a lot of certifications, and they may have the greatest personality on earth.

And somebody will say, well, I want to hire them. They seem awesome and let, but let's make sure they can actually do the job. And so, We have [00:37:00] live attack exercises on the range, and this is all virtual, by the way. Our, our ranges are all, you log in through a browser somebody gets in there and they actually have to perform exercise.

You know, just like a SOC analyst would do, for example. They're logging into their SIEM, they're looking at alerts, they're doing investigations or whatever it is that the job is for which they're being considered. They are doing that job in a simulation and. The manager is able to see how well they do.

They're either going to do really crappy really well, or somewhere in between. And the somewhere in between is most likely. And that gives them a plan for moving forward. Cause remember, we already like the person they already have lots of certifications and they already have the will. And so now we have a learning plan for them to go off of.

[00:37:44] **G Mark Hardy:** So it's almost like trying out for the softball team. We can get out there and you're not actually playing a game against another school, but you're saying, I want to do this. So the coach says, all right, let's see what you can hit. Let's see what you can throw. Let's see if you can field. And you go do these things and then they go, wow.

And I suppose, as you [00:38:00] mentioned, it could be internally for being able to identify other talent, and it's always been the case, is that you need to look laterally. I remember. A few years back and I need to put, look up the reference on this to make sure I get it correctly. Cause I hate dealing with urban legends but as I recall, I think it was in the UK when they had a national cyber challenge and the person who won it was like parking lot attendant or something like that.

It just had never realized professionally what this person could do, but was amazing because I was go home at night and they just do this all day long and it's like, you should be here and, and things like that. So we could use that also potentially for recruiting and, and get them on a range and maybe have a bunch of college graduates or soon to be graduates and say, Hey, you could be able to help score their abilities. And they might even be able to use that to come and say, Hey, here's my range scores. Almost like being able to say, here's my SAT scores.

[00:38:51] **Debbie Gordon:** we call it game film. So just like coaches look at people playing game film and something else I want to expand on that you said about, you know, the person who was a parking lot attendant [00:39:00] who is really great at cyber cause they do it for fun. This type of so ranges help lay level the playing field.

So as we look at growing the cyber workforce and giving people opportunity that would never think that they would get into cyber, whether, you know, whether it's, you know, women or other underrepresented communities and populations who may not have gone to college. And yet they're really good at something.

These range assessments are able to level the playing field because it doesn't matter what gender you are, what color you are, what background you have, if you can go through this and do it, that's proof and that's better than any certification.

[00:39:39] **G Mark Hardy:** And that's very, very good insight. We have to make sure we're not, you know, so strict. And again, I'd read someplace where he said, you look at most of these. Job ads and like 80 or 90% of them require some sort of a degree. But the reality is, is a lot of the people don't have it, don't need it. And then we get a little bit well, I've got my degree, so everybody else should have to do it.

It's like, [00:40:00] no, that's the stuff you learn there is not going to help you over here. Operationally and putting somebody in the, in the, if you will, at the keyboard and said, all right, go fight and see what you do and go deal with it. A person can walk away and, and as you said, doesn't matter about their background, their color, their race, or their gender or whatever.

Are you good?

And then can you be part of this team?

[00:40:21] **Debbie Gordon:** And we're seeing a lot of companies lift the degree requirements because they're, they're just there because they've been there.

[00:40:28] **G Mark Hardy:** right. We've always done it that way,

[00:40:29] **Debbie Gordon:** exactly. and and they have to they have to see the impact of it, that they're alienating so many potential very qualified candidates.

[00:40:37] **G Mark Hardy:** And, and, and I think that's quite good. And, and many times later in life, people said, Hey, I want to go back and backfill that educational opportunity. And if they got a regular job with benefits, it makes it a whole lot easier to do so. Well, we're getting close to the end of our show here, and then we, we've covered a whole range of topics and things like that.

But any lessons learned that you'd think of from the CISOs who may have come through the range and said, wow, I'm so glad I did [00:41:00] that. Look what I came away with that I didn't have before.

[00:41:03] **Debbie Gordon:** I, I love seeing this. We make their jobs easier because there's a lot of elements of range exercises that's, you know, managerial and team building besides the technical part, but security leaders don't know what people are supposed to learn. That's not, it's, it's this whole other area.

You know, not only did they not sign up to, to manage soft skills, but they also didn't sign up to manage, you know, learning and development of their, of their team specifically. And so this makes their job easier because we're able to conduct these simulations and more importantly, give them the reports and the observations that our attack masters who are facilitating the virtual exercises can give them.

And there's so much great insight there that it takes a burden off of the CISOs and that that's a really cool thing because everyone is so busy. And it also helps them. Check the box of a strategic priority. And what I mean by that is think about going to the [00:42:00] gym. You never like have all this time to go to the gym.

You have to make time. At least I do. And if it's not scheduled, I'm not going to find time, because it doesn't exist. Same thing with training. You have to schedule it and plan it and make it a priority, otherwise you're never going to get to it. So, once we, when we work with companies. And we get all these simulations scheduled.

It's, it's very much, it's very liberating for these CISOs because then they don't have to worry about, they know it's taken care of. They have the whole year planned out. It's, it's done.

[00:42:28] **G Mark Hardy:** Wow. That's really great stuff. And, and well, Debbie's been a pleasure having on the show and, and, and thank you for your time and everything you shared with us and for. As remember, if you want a Polish security program, you need good policies, you need practice, and of

course you'll need proof. And the way you can improve each of these things is through testing at a range. because ranges are going to provide expertise, education, and an ability to demonstrate whether. The person's new whether experience, whether they're coming from some other part of the organization. And they're really kind of a proxy for risk assessment [00:43:00] because they allow you to take the problems that you might encounter in real life and test and go through them and make sure that your team knows how to minimize those issues before they actually face them in real life.

So if you want to improve your cloud and your cyber capabilities get to a range. So for audience, thank again for listening today's show if you like please go ahead and follow us on your favorite podcast channel. Follow us on LinkedIn. Check out on YouTube and follow us there. And if you love listening to us at work, it's great or working out.

As you said this, we time these episodes to last about as long as a good 45 minute workout or a drive into work. Debbie, any last thoughts? Any if somebody had further questions for you, how are they get in touch with you?

[00:43:36] **Debbie Gordon:** Yeah, thanks G Mark. Our website

is www.cloudrangecyber.com so we are a virtual cyber range. You don't have to go anywhere. And it's all it's all consumption based. Very flexible for any size team. Or you can send an email to info@cloudrangecyber.com or follow us on LinkedIn or the socials and look forward to hearing from you.

[00:43:59] **G Mark Hardy:** Well, [00:44:00] awesome. This has been great. So for everyone out there, thank you for your time and your interests. This is your co-host, G Mark Hardy, and until next time, stay safe out there.