#153 - Game-Based Learning (with Andy Serwin & Eric Basu)

[00:00:00]

[00:00:00] **G Mark Hardy:** Hello and welcome to another episode of CISO Tradecraft, the podcast that provides you with the information, knowledge, and wisdom to be a more effective cybersecurity leader. My name is G Mark Hardy. I'm your host for today. And I have with me two excellent speakers and some fascinating folks, Eric Basu and Andy Serwin. Eric and Andy, welcome to the show.

[00:00:32] **Eric Basu:** Thanks, G Mark.

[00:00:33] **Andy Serwin:** Thank you.

[00:00:33] **G Mark Hardy:** before we get going, I want to share a quick word from our sponsor, Risk3Sixty It's a cybersecurity technology and consulting firm that works with high growth technology firms to help leaders build, manage, and certify security, privacy, and compliance programs. They publish weekly thought leadership, webinars, resource like... PCI Compliance Program Workbook, their Business Case for SOC 2, and ISO 27001, the Path to Certification, and many more titles, [00:01:00] all available for download at no charge at Risk3Sixty.Com/Resources. Let Risk3Sixty help you build your business case to achieve certification compliance. That's Risk3Sixty.Com/Resources.

Anyway, back to our, presentation, gentlemen, thanks for, for being part of this. , we talked a couple of times back and forth over the last few, it's been a couple of months now prior to this and,, want to get into some areas that, , I think our audience will find fascinating, but quickly, if you don't mind, could we, do some quick self introductions?

, Eric, let's start with you.

[00:01:33] **Eric Basu:** Sure. Eric Basu. My first career was as an officer on the SEAL teams. I got out, worked in consulting firms, started my first company, Sentec Global, in 2001. We were a defense contractor. We did a lot of cybersecurity services, engineering services work. I sold that company in July of 2021 to Deloitte, and I immediately started Haiku.

At Haiku, we create Games that teach cyber [00:02:00] security. So it's called game based training, alternatively, serious games. But it, they're actual games that teach cyber security and those games are based on two principles. One is that, , a good video game can get your brain in the flow state within 15 minutes. And the second is a 10 year study by McKinsey that shows that when your brain is in the flow state, you're 500 percent more likely to be able to assimilate. And, yeah, that's me.

[00:02:23] **G Mark Hardy:** And that's fascinating. We're going to get into those details in just a little bit. Andy Serwin, welcome to the show. And tell us a little bit about yourself, please.

[00:02:31] **Andy Serwin:** Thank you, Andy Sherwin. I'm, , an attorney, , by day, so a partner and global co chair of a privacy and cybersecurity group. And I've been doing that for about, , 28 years now, and I've worked on a lot of the major breaches you've heard of, as well as a lot of remediations and, pre incident planning.

, also serve on several boards, , of directors and, , serve as chairman of the board of the NCFTA, which is a public private partnership in Pittsburgh that works very closely with law enforcement and, other agencies. to try to promote cyber awareness. So thrilled to be here [00:03:00] today.

[00:03:00] **G Mark Hardy:** And I have my NCFTA disruption coin right here on my desk

so thank you very much for being part of the show. So let me start out with Eric a little bit, because you had mentioned about the game idea and gamification, how it's gonna be much more effective for people, for learners to get into the flow and things like that. How did you get the idea about getting into this line of work? And what was it that made you think, Hey, we're onto something?

[00:03:21] **Eric Basu:** Yeah, I mean, it's, it's interesting. It was definitely a process, G Mark. so I've played video games since Pong came out in the 70s to date myself. And then as my kids have grown up, I've played with them thousands and thousands, maybe even more than that, of hours in video games. And I've always been fascinated with the fact that video games teach us.

And for anybody that plays video games or has kids that plays video games, you see that. Somebody playing Elder Scrolls and there's a very complex potion making system or, you know, a race card game where you've got to master these

controls or even a first person shooter. The video games have a way in which they teach you, and that's a very mature technology.

You know, video games have been around, you know, for almost or maybe slightly over 50 years, and [00:04:00] we've developed ways in which to get the video games to work with you. And Jane McGonigal is the one in her book, Reality's Broken, who wrote that a good video game gets your brain in the flow state in 15 minutes. And that's different from any anything else you do. You're not going to start playing piano and get the flow state in 15 minutes unless you're Mozart, right? But a good video game will. That's one of the reasons it's so addicting. So the science behind video games and getting them to get your brain in that flow state And then taking the fact that you're in the flow state and employing, we use learning engineering techniques that were pioneered by Carnegie Mellon's University's Human Computer Interaction Institute.

You see them in products like Duolingo. Be able to get people to learn while they're in the flow state, but instead of learning a potion making system, you're learning Linux commands. You're learning SQL injection. You're learning, you know, the specific rules that the SEC has for when you have to notify them in case of a cyber breach.

We're teaching things that fundamentally aren't fun or interesting, but we're doing them in a context where your brain has been brought into the flow state. And, [00:05:00] so I came up with the idea, when I sold, my last company is that I wanted to have a way to give people hands on skills that they can actually demonstrate to employers. And I first thought about the idea about eight years ago or so, maybe a little bit more than that, when there were no cyber ranges available for individuals. By the time I sold my last company, there was hack the box, try hack me, you know, plenty of cyber ranges out there. And so I looked very carefully at what they did good and what they did badly.

What they did well is, you know, had a consumer price cyber range where you can go test your skills and go to hack the box range. Again, they tried to get in the top 1 percent of TriHackMe. What they didn't do well is changing the way in which you learn. A cyber range will test what you already know. So I'm going to go into HackTheBox injection, range. It's going to test whether I know how to do SQL injection because I have to do it in order to be able to get root and cut and paste the flag, right? But the range itself doesn't teach me how to do it. It just tests whether I can do it. In order to learn how to do SQL injection, I've got to read their PDF or watch their video. Old school ways of learning, right? [00:06:00] It's reading, or it's watching an instructor. These are, there's nothing new about those ways of learning. And those are the ways of learning that really

are kind of struggling to meet the cybersecurity workforce demand. Because they're still too hard for many people. So the people that are naturally drawn to the cybersecurity STEM curricula are the ones who are normally drawn to it, right? Same kid that would have taken apart a transistor radio and put it back together naturally gravitates towards this and does very well. The person who may be more visually, more creative, you know, creative oriented who is not naturally drawn to this is intimidated when you put them in front of a command prompt or give them something that looks, you know, like a hard STEM curricula.

And so we draw in a number of those other people helping to increase diversity in cybersecurity.

[00:06:42] **G Mark Hardy:** That's interesting, because what we're talking about then is different learning styles, where somebody could be tactile, where they actually have to do something with their hands, somebody's auditory, somebody is visual. What we're finding in the concept of a gamification is that even if the subject itself may be relatively boring or dry, [00:07:00] to quote Marsha McLuhan, the medium is a message.

It's the way that that is delivered and that then creates something that's consumable and is desired to be consumable. By, the individual who's actually going to be doing the training. And now by doing a little bit of intelligent application of this, instead of teaching something, and oh, by the way, I think you mentioned Duolingo and I'm using Duolingo.

I'm going through it. And, so

far so good. I just finished the top of my league this past week. And of course it says, here's another one, but yeah, the gamification works. And it, even for me, as an older guy, it's like. But yeah, I just want to get one more thing you want to, want to push at it. So there's no question why that was psychologically. Now over to Andy, because I'm aware you probably are the most expensive per hour gentleman I've ever had on my show. If I wanted you to board of directors, I understand. I don't know if you want to mention numbers on the show, but it was a pretty impressive, and probably worth every penny of it too, if I wanted to bring in for four hours to brief a board, but, let's jump over to you a little bit because I know we have some time constraints on that.

[00:07:54] **Andy Serwin:** Yeah, no. And look, I think when you look at, you have similar issues with the boards and [00:08:00] training them, right? And so I think part of this is how do you meet the board where they're at? And I think

what we what I see a lot is the subject matter experts do a very good job managing the day to day kind of root causes of cyber and that, but the boards are never going to be that technical, nor can we expect them to be.

And so part of this is training the board to understand the context of these risks, which is important. And then part of it is, I think one of the changes we're going to have to do is start training the technical people on what the board's obligations are, how the board speaks, and to pick on the Up on the Duolingo thing, the board uses different language than the security people, the security people use different language than the privacy people, and I think that's one of the really attractive things about Haiku is.

We do have, we have a skillset issue, but we also have a language issue. And part of this is having all of these different stakeholders learn each other's language so that they can communicate better and actually understand the risks they're taking, manage the risks better, govern them better, and then, you know, have less surprises [00:09:00] because that's what you really don't want is.

The board being surprised, down the road by something because, you know, someone spoke in one language and they understand a different one. And so I think that's really one of the key things where, you know, I think Eric's company is unique is he has gamified this. And, you know, I, I, we do folks tend to focus on skills.

I don't think you can discount the language issue. And I think it's a critical issue that we have to deal with going forward as a profession.

[00:09:24] **G Mark Hardy:** And I think you've raised an excellent point there is that it's a language in the communication is oftentimes CISOs and security leaders tend to come up from a technical background, and they'll express things in bits and bytes and using all kinds of terminology when in fact the decision makers that they're dealing with.

Particularly at the board level are going to be focused at the strategic level. They're not even operational. They're not trying to do the day to day stuff, but where do we want to be in six months or a year? How do we deal with compliance? How do we manage the overall risk to the organization? And where does that risk come from?

And are we mitigating it effectively utilizing the capabilities that are available to the organization?[00:10:00] What I do find kind of interesting in combining the thoughts from the two gentlemen is that I think of gamification for a board of

directors. Does that work? Is that trying to teach an old dog new trick, so to speak, or as I had observed myself, you kind of get into it and you go with the flow. What's been your experience so far?

[00:10:18] **Eric Basu:** So that's actually a really good question. And by the way, I actually differ, in gamification from game based, and that my, my, my difference, and I got to say, I'm probably the one that mainly is the, you know, I'm cognizant of the difference, but I've written a number of white papers on it, is that gamification is when you take something that is, Well, by definition, not gamified, right? So you'll take a cyber range or a powerpoint or a video and then you put a leaderboard on it You put some badges on it or you put some graphics in a cut scene But the gamification doesn't change the way in which the training is delivered, right? You're still watching the powerpoint doing the range watching the video And the gamification is designed to make you more likely to do that, but it's not designed to actually change the way in which you learn. Game [00:11:00] based means we're actually changing the way in which you learn. I mean, you're not going to be watching that video or doing the cyber range. You're going to be playing the game, interacting with all the best practices of a video game. So I've actually written a few white papers on game based versus gamification. Interestingly, the number one people who are reading my white papers are our competitors. I can see it on LinkedIn when I, when I look at them, it's kind of funny. So we actually, one of our customers, is a large private equity firm. The CISO actually said to me, it's interesting. We're building a security awareness product.

He said for the security awareness product and the products you're aiming at the board, they will not. Play the video game as it is right now. It's too cyberpunk edgy. It's too, he said, my IT people love it because they all play video games. As another CISO said, it's not, does your cyber security team play video games?

It's which ones do they play and how often? That's the question, right? It's their golf. But he said, board members typically don't video games. Nothing said. Games are... across all mediums, right? Everybody, including [00:12:00] septuagenarians, octogenarians, even nonagenarians, play games of some sort. It may be a crossword puzzle.

It may be, you know, a sudoku. It may be something else, but they all play games. And so the question is what game appeals to that particular demographic? And I actually had an investor ask me this and said, when you're looking at a new a new area like security awareness, we're building products in that, which hopefully not what we should have released in a very short time. He said, you aren't looking at the content you're producing, you're looking at the

type of game that you develop. And I said, exactly. He said, why is that? I said, what is new in security awareness? There's nothing new. You aren't going out there trying to teach zero days. You're trying to keep people from the same phishing attacks that they've been falling for the last 10 years. I said, so there's no new content we're putting out there. It's the way in which the content is delivered to interact with the user's mind to get them to both increase their adoption, their engagement, and their information retention. That is the key. That's why the type of game you have is completely different.

And so for board members, we have [00:13:00] a different type of game. It's a different look. It's a different feel. And, for security awareness, we have a different type of, game that appeals to everybody. And so I'm not going to tell you on this one, but, you know, stand by in a few months and you'll be able to see it be released. But you'll see that we don't just do one type of game. We're not a one trick pony where we, oh, you've got a cyberpunk role playing game. No, we've got a variety of different games. But the games are used to deliver the information.

[00:13:22] **G Mark Hardy:** Got it. So, I want to go a little bit more into that, but again, I want to go back to Andy if I may. Because you brought up a couple of things. We're talking about boards and what they need to understand and things like that. For the CISO perspective, we're looking for, you know, what are the parameters in which we can operate?

As an attorney, you've read things that, for example, it was about a year ago this month that Joe Sullivan received a sentence for a 50, 000 fine and three years of probation. And for those who don't recognize the name, Joe was the CISO of Uber, and it was strange that all of a sudden we're thinking that as a CISO, you're going to be served a well's notice and then potentially held criminally liable for actions and decisions that most [00:14:00] logically should have been done much higher levels of the organization beyond the CISO acting.

independently without authorization or supervision. So when we deal with things such as that, what insight do you have for CISOs and maybe their ability to communicate situations to their executive team or even the board when a high risk event occurs and then. Is there, you're not really a whistleblower, but do you almost have a duty to say, that's an unlawful order, I'm not going to go ahead and click send?

What are your thoughts on that?

[00:14:30] **Andy Serwin:** Yeah, no, look, I think when you really boil a lot of these duties down, there's a duty to have the right systems in place to find material or red flag issues, right? Mission critical issues. And then there's, as an officer of a corporation, there's a duty to act on it, right? And there's, Also a duty to escalate.

And so I think that's really where things can get you can have it go sideways in any one of those three. Now you can have all three, but if you don't have the right systems, you're flying blind. If you don't have the right [00:15:00] escalations, the people above you don't understand it. And if you're not, fixing the red flag problems you have, you're not doing your job.

I mean, it really is that simple. And so where, the Sullivan case was an interesting one. There was a, Consent decree in play in that one. And so they were in a bit of a unique position about what they did or didn't have to disclose to government agencies that, many companies aren't, but it still illustrates the point that I think.

Whether he felt he communicated clearly or not, it sounds like the board maybe didn't understand what he was saying. If he did say something, I don't know what, I wasn't privy to those conversations, but that's the issue, right? If it's not, we can no longer, I think, as subject matter experts, expect boards to understand the technical laden jargon that we go to them with, if we actually want them.

You know, one, to be able to oversee these companies, but two, and I think this is a conversation I've had with a lot of CISOs and CPOs. They're the ones who have a lot of input on your budget, as well as the C suite, and if they don't understand what you do, [00:16:00] it's hard to get funding for a lot of the things you do want to do, and so it's in everyone's interest to have...

Full and frank discussion about the risks the company's taking, what risks the company should be taking. I mean, this is business. It's not kindergarten, there's businesses take risks. That's part of the deal, but you want everyone to be aligned. And we've created actually this little grid, which sounds stupid, but it's color coded, right?

And what I always tell clients is it's great to be in the green, which is, Low risk, high value. It's fine to be in high risk, high value. If you know what you're doing, low risk, low value, you know, maybe you do that. What you don't want is high risk and low value, right? Because that's exactly where companies make mistakes.

And if you're, you know, and I think it goes to your point of like, if that's the choice, everyone just be there, be really clear about that's the choice. And if you're speaking different languages or different dialects of languages, It's hard sometimes to understand you're playing in that red box.

[00:16:54] **G Mark Hardy:** So, if you want to stay out of the red box as a CISO, and you're finding that there's communications difficulties [00:17:00] with your board, who ultimately have a fiduciary duty, it kind of rolls back, does a CISO have a fiduciary duty to the organization? In so far as the board does, or is it just pretty much a matter of just staying

[00:17:11] **Andy Serwin:** No, usually they're officers of the corporation. So they have, you know, they have a duty of, of care and, you know, they also have the duty of loyalty, but their, their duty of loyalty isn't necessarily as focused on, you know, the oversight that the board is because the board's role is obviously. The oversight side of this, but they do, they still do have that duty as well.

But yeah, I mean, most CISOs are at a, at a level of a company where they would be fiduciary officers. And so, you know, you, you can have a debate as to whether the board should learn more about what the CISO does versus the CISO learning more about the board. The reality is boards. Having served on them, while cyber is a critical risk for most companies, it is in no way the only risk, right?

And so what we try to tell boards and we try to tell subject matter experts is Align to the Delaware fiduciary duties because those are the constant, right? [00:18:00] Environmental risk has different language than, you know, privacy or cyber. But if you can all align to the one thing we all know we have to deal with, which is Delaware fiduciary duties in most cases for the Fortune 500.

It just makes life easier. And it's the context around it, right? You're not going to change. This is the EDR we use, but you are going to say, the reason we use EDR is to protect these five business processes that are critical to our company. And as a result, this is why I need you to fund X. That's a different conversation than we use X company or Y company.

And I think that tends to be that. And look again, I think that's where. Eric's company really, offers a tremendous value as it can start to build those bridges between these different functions. Oh,

[00:18:41] **G Mark Hardy:** And Eric, I'm not ignoring you, but I'm aware Andy has a hard stop in about five minutes to get to another call. So, a question

with respect to, as you say, the communications and up to the board and things like that, is that, if the message is not getting through, And you see that the organization is straying into a dangerous [00:19:00] situation.

What do you advise a CISO to do? I mean, do they lawyer up? Do they just simply go ahead and start jumping up and down and make noise? Do they back off, resign, update their resume? Not every time will you find out that senior executives will do what the technical person thinks is best, but the board has other data, and it might be in fact a superior decision.

How do you help CISOs Live with the fact when they walk out of a boardroom saying they didn't get it. Any, any thoughts on how that might communicate, Andy?

[00:19:24] **Andy Serwin:** I think you've got to display the red flag. I mean, that's what you have to do. And then I think you get to a place of saying, if you have, you know, I think at the end of the day, the CISO is an enterprise level executive, but not the same way, you know, a general counsel might be.

Or, you know, a CEO, and so ultimately, it's not the CISO's call, but they've got to make it clear and look if they feel that that really impedes their ability to do their job, then that's a different discussion. But I think that what I tend to see more is not CISO saying, here's the risk [00:20:00] really, really red don't do this. It's, they're saying it in their head, but It isn't communicated in language the board understands. And I think until you do that, you know, leaving the company or doing something else probably isn't the right call. It's, you've got to make sure you as the professional have communicated the risk in clear, unambiguous terms to then say, okay, if you're not going to do it, then I have to make a different choice.

[00:20:24] **G Mark Hardy:** Got it. And so what we have then is a situation where you don't want to have a CISO or somebody in a security leadership position withholding information from a senior level. At some point, though, you have a squelch on there. You're not going to worry about 10 cents or 20 cents or whatever, you know, that doesn't get reported. But

[00:20:40] **Andy Serwin:** You go to materiality or you go to, you know, mission critical status, right? And that's the thing is not every risk is that

[00:20:47] **G Mark Hardy:** Right. And now we're into the SEC ruling about materiality and their whole ruling that came out this past month, or actually effective this past month, with respect to boards. Do you think the SEC is going

to double down on that and require boards to report on [00:21:00] cybersecurity expertise in the near future, or do you think they're just going to let their current ruling stand?

[00:21:04] **Andy Serwin:** think they're going to let it stand. And I, you know, at some level, look, I hope they do, because I think again, if, if we can't put cyber in terms that a normal board can understand without deep cyber expertise. I think we as a security profession have failed, right? I mean, I think that's kind of part of it, which is it's not that you don't want people with cyber security experience on boards.

But again, if these are enterprise risks that are framed in Delaware fiduciary duties, which I believe they are, boards do that all day, every day. So part of this is getting boards to understand context. This isn't just a CISO problem. Be very clear. They've got to understand context for risk, and then the CISOs have to align.

They're reporting to that context, and if we can do that, I think you fix the problem, which is boards understand it, and there's better public disclosure, whether or not you have, you know, five CISOs on your board, right? And I think, could you? Sure, but I think that's probably part of the reason the SEC didn't quite go as far as they could have, because I [00:22:00] think they probably saw that this is the sort of enterprise level risk that impacts everything.

[00:22:04] **G Mark Hardy:** Got it. And so back to Eric now, as we take a look at some of the solution that you guys have been developing. Yep, didn't forget about you. Is that both for allowing for the game based learning for the technical staff and also at the board level, what you're doing then is you're kind of creating sort of a common language, so to speak, even if it's approaching from a different perspective, because at the end of the day, we're humans. And humans have certain inputs and outputs and things like that. So really, you've been able to adapt to that. How much of that information that you are working with would be generic? That is to say, everybody has to do the same thing. For example, if you're trying to conform with some NIST standard or some ISO, you can get that out of a box.

Or how much of that becomes custom? And then how do you deal with somebody who says, I have some custom requirements, and I'd like to go ahead and turn that into a game based learning. Is that something you guys can do? And if so, how does that work?

[00:22:54] **Eric Basu:** So we actually created something called, we call it FORGE, it's the brand for it. So basically, it's something our [00:23:00] developers developed to make their jobs easier, but it's a drag and drop, no code way for anybody to be able to create their own, game based training. And so, what we found in early deployments of this is that it reduces the cost of developing the training. And, and the time frame by about one tenth. It reduces it to about one tenth, not reduce it by one tenth,

it reduces it to one tenth. Yeah, yeah, yeah. It's a big, big change instead of small change. And so, I mean, you know, we're working on, with one of the major, certification providers on developing a game based training for their certification using Forge.

And we did the first module, which normally would take about probably a month to a month and a half. We did up the first iteration of it in two days. And, now it's still required quality control and some going back, but I mean, the first version of it was done in two days and, and actually when my, content, leader told me that I said, how in the, I was expecting two weeks.

He goes, no, it's actually really easy to do. So with the forge platform, anybody can go in there and they can develop their own no code training. And so, and the no code training isn't just for the hands on [00:24:00] skills. We were just talking with, a group earlier, based out of Florida and they said, well, we need training that is. From very early on high school students to very advanced, and I said you can do that, you can create something and you can do it within, you know, two weeks if you want to. Game based training. So this isn't creating a PowerPoint or a video or a CyberEdge, it's creating actual game based training that's going to be an actual game that you get.

You get all the benefits of the game based training and you get all the benefits in the back end of measuring all the skills to the NICE framework. But you can do this within a week. And you can build one that's very simple. How am I going to teach high school students the basic cybersecurity hygiene? On the other hand, for the advanced folks, you say, I want to actually go through an extremely detailed and complex SQL injection attack and defend. How do they both attack against it and defend against it? And this is going to be a competition. I don't want to set that up. You can set them both up in the exact same platform.

[00:24:51] **G Mark Hardy:** Interesting. So have you found then your preliminary results that you had more engagement with people that they tend to return to the training more frequently [00:25:00] than they're absolutely required to do?

[00:25:02] **Eric Basu:** Yeah, what's really interesting, the stats I've seen on like online video training for cyber security or anything is that 90 percent drop off rate after three months. People stop after three months. On Duolingo, I am, ten days away from getting my 365 day challenge, which makes me feel good until I see people that have done 720 day streaks in there. And I'm like, you bastards. The, you know, you just

[00:25:22] **G Mark Hardy:** And I'm thinking, why haven't you mastered it in 365 days? You got to keep going back.

[00:25:28] **Eric Basu:** I, I I know. So, and that's the advantage. We have a 20 percent drop off rate, and so compare that to 90%. You can say, oh my God, 20 percent people drop off. I'm like, compared to 90%, our adoption rate's far higher. Our retention rate is higher. I mean, game based training, once people get into the game, they continue to play the game.

And as long as they continue to see value and they really, they keep coming back.

[00:25:49] **G Mark Hardy:** So Eric, if an organization says, Hey, I, this makes sense. There's different types of learning. We could do, there's a static learning. That's going to say, I got to comply with some compliance requirement or [00:26:00] government program or whatever. And then that's going to be fairly static content. We also have more dynamic content, which could be based around an organization's specific requirements and things such as that you'd mentioned that the, the concept of a FORGE tool, which is non programming, you can make things and then it'll all be customized.

Does every. Kind of game based thing end up the same. And are you always Zelda? And you just have a different, how, how does this actually play out?

[00:26:25] **Eric Basu:** So yeah, it's interesting. We actually had to change some of the characters in there so that they're less gamey. And so people have the option to have, you know, it's set in the conventional world and you have your CISO and you have your CEO characters and you have, and they, and they, and they look, you know, different.

It's still, you know, it's not, it's not boring, but it's, you know, simply more accessible, I think, to people that. Aren't interested in, you know, cyberpunk or fantasy sorts of things, but the different types of games are really what you want to make of them. Right. So, I mean, using the forge tool, you can build a, game that is very heavily information oriented, for example, it's, you know, I want this

[00:27:00] to be very heavily talking about. So that's why we could actually build a training program for CISSP. You wouldn't be able to, for example, build a cyber range that teaches CISSP. I guess you kind of could, but it's so process oriented, you kind of wonder why am I sitting here poking around in a cyber range for, because 90 percent of what I need to know is actually knowledge based rather than technology based, right?

So you can do that in Forge if you want. If you want to create something that's purely knowledge based, like a CISSP, which is something we have in our, in our queue, track, you can go ahead and do that. If you want to do something that's extremely technical, you can do that. If you want to do something that is a back and forth, repetitive, okay, do this.

Now I've got a timer. Now do this. Now do that. You could do that. You can change the type of training that you do. And then you can also, configure it to whatever you want. Like we have one of our, clients said, I bring in help desk people and they, don't have the basics of cyber security.

Can I create, use Forge to create something that basically gets them up to the very basics in cybersecurity so they [00:28:00] can be a better helpdesk person? And I can actually evaluate them as I look at their skills on the back end and how they're doing, see how well they can move into our SOC analyst type of roles.

And so, something very easy to do, and once you create something in Forge, you can create a template. So we can take, like, we're building one for the ISC 2 CC. You can take that template, you can go ahead and move it over and say, okay, use this as the basis for your help desk, because it gives them a very strong basis.

And then you can add in the specific technologies, the specific processes, the things they need to know. Same thing with what Andy is talking about. We're building a capability to be able to train IT staff on when do they need to notify the executive staff and the board about things that could be potential SEC violations.

No IT staff. Anywhere, I would guarantee you knows that right now because the rule has just changed and there's no training that exists on that and Nor is there, you know, I don't send somebody to a SANS course for weakness Okay Now I want you to tell me whenever there are breaches that require SEC [00:29:00] notification.

They'll shrug their shoulders and go I don't know. I just went to a CEH course. How would I know that? You know, I went to a SOC analyst course. How, how, how do I know these things? Because there's no training on it. We actually are building training specifically for that aimed at trying to increase the risk resiliency of the organization overall.

So if they can look at and through the admin panel, they can actually look and go, here are the people that have trained. Here's how well they've trained. Here's an idea as to what my training risks, the training impact on my risk resiliency is.

[00:29:27] **G Mark Hardy:** So a couple of ideas came to mind. I'm making notes here as they go. The first one might be the easier one is, is we talk about training and awareness and getting things like that. And you know, the typical go to organization would be a security awareness company, whether it's KnowBe4 or PhishMe or Wombat.

I'm not going to leave anybody out because they don't know the whole list, but we get the general category of company and we might say, well, that's. Yeah, I'm close enough for government work, so to speak, but the reality is if you've been able to demonstrate increased effectiveness through doing the game base, and if [00:30:00] so, what's that value proposition that you can then give to a CISO who can take to his executive team and said, Hey, I want to buy this because here's what it's going to do for us right now.

We've just been doing the same thing and, nothing wrong with companies that are out there. But I remember when I was in the military, we always had to do an anti terrorism training or something like that. It was security awareness, but it was physical security awareness.

It was the same video every year. You would get into the same airport and you got the same rental car and he had the same cardboard box behind the wheel and the same person knocked on your door and then, and everything else. And after a while, it was just like a memory test. You did this once every 365 days.

So, you know, question one is differentiation with a existing training company. Is there a threshold below which you say, yeah, that's fine. That's let's do it, cheap and easy, but above what level would you help a CISO justify? We need a more effective tool such as the one that you have.

[00:30:54] **Eric Basu:** So it's interesting. I've done a number of, speaking engagements and. It's been at least a half [00:31:00] dozen, maybe more, opportunities, incidents where CISOs came up to me after I was speaking and

said, I love what you're doing for cybersecurity career skills. Can you do the same thing for cybersecurity awareness training?

Because my employees hate it. They despise it. I mean, they refuse to do it. the worst example I saw was, one of our, Navy customers who they have actually a program in place. I don't know what it is, an application. Nobody does it. So every quarter they get everybody and they do different all hands meetings, dozens of separate all hands meetings with 50 or a hundred people in a room.

They show them a PowerPoint, which is the exact thing you said. It's the same thing they've had for the last 10 years. Boring. And they just force everybody to sit in there. They put their names on a, on a list, and then they check them off in the application to say that they did the training. So, I mean, they have an application.

They spent probably millions and millions of dollars on. Nobody does it. They force people to go to an all hands because in the military you can do that, and then they check their names off manually. That's the worst example I've seen, and they said the same thing. Can you give us training that my people actually [00:32:00] want to do?

And all the best CISOs, which is actually all the ones I've talked to, all said the exact same thing. It's not just that I want them to do it. I want them to actually make a difference in what they do. And so we have a couple of modules coming out for security awareness that are exactly that. They're things that are fun and that people want to do.

And you have some gamification features in there. Like you've got leaderboards and they can compete against other people in the company. Those are the gamification features. But the actual games themselves are things that people might want to do. One of them is a mobile app that is things that people actually might want to do on their own time or give them time to do it at work.

And now we're talking about continuous training instead of the intermittent training. And So, continuous training is something that, you know, the people are doing it all the time and they're building up their profile on the back end and as a CISO, you're just kind of looking at the admin panel on the back end and going, okay, we're getting a lot more engagement in the security training than I expected.

hopefully not too much where they're spending four hours a day on a workday, you know, actually doing the games instead of doing other things, but that's a

problem that we'd like to have, right? That's a champagne problem where you can now, [00:33:00] you can one monitor them and have them, Decrease, but you know that your people are getting better at what they're doing because they're spending so much time doing it And if they're spending that much time doing it, they're definitely assimilating Right?

They're definitely learning better how to avoid that phishing attack. When I guarantee you, you just throw them in a room and you force them to watch a PowerPoint, they are no better when they left there. Maybe even worse because they're, you know, maybe a little passive aggressive and resistant to the fact that this is being forced down their throats as opposed to they've got a game on their phone that they're doing with the, their coworkers and going, this is actually an awful lot of fun.

You know, this is almost a guilty pleasure, again, not even aware of it. One of the best examples I've seen for getting in the flow is actually an example. We're working with the Girl Scouts of San Diego to give them their cybersecurity merit badge using a very basic module in our game. And so we had a group of girls come up to our station.

One of them was probably 10 and the first words out of her mouth were, I'm no good at math, right? Which is kind of cute and kind of funny. 45 minutes later, she's arguing about whether one of the robots in the game was cuter than the other robot with one of the other girls. But she's completely [00:34:00] unaware of the fact.

She, if, she knows command line Linux. I could put her in a Linux terminal and say, hey, can you list out what's in there? And she would type LS. Can you change to the root? She'll see the, you know, um, dot dot. Um, can you tell me what's in that file? She would type cat. Completely unaware of that because she was in the flow state, just enjoying the game and the characters and all that.

And this is what you want your employees to be doing to come back to the point is that you want them to be sitting there going, Hey, you know, I, you know, really kicked your butt in that game we did, you know, earlier during lunch, completely unaware of the fact they're probably not going to fall for any of the basic phishing scams because they know exactly what they look like.

[00:34:35] **G Mark Hardy:** So, another thought occurred to me, and again, I still get to the next one here, but I've been to conferences where they have CTFs, capture the flags, where everybody comes in there and you can, in the

evenings or whatever, you all sit down and go to terminal, grab an adult beverage, and then just start bang, tack, tack, tack, tack, hacking away.

That's sort of gamification in a way, but really you're not using the game based learning because you're just there at the keyboard doing the Linux [00:35:00] commands because you're trying to get into the Linux box. For example, do you see an application for this type of educational use for a highly technical team who may already be comfortable at command line?

And what is it that you do differently that's going to make people gravitate to that instead of just sit down there and just bang away at the keyboard?

[00:35:20] **Eric Basu:** Yeah, so here's a great example. I was at in the Luxor. I live in Las Vegas. I was in the Luxor Esports Arena two years ago at Black Hat for, um, one of the competitions they had. And so it's a beautiful arena, You know, can hold probably about two or 300 people. There was maybe five people sitting in the stands.

And so, you know, they had a number of teams, very accomplished teams, and they had two announcers. And one of the announcers said, Oh, they're doing a cross site scripting attack, cross site scripting attack. And I looked at it and I studied really hard and I'm like. Yeah, I guess they are. None of it is interesting or exciting, right?

And I'm actually in the industry. There's nothing exciting or interesting about this. There's no, you know, you're not going to be [00:36:00] Twitch streaming this to an audience of a million people. Nobody cares. It's, it's about as boring as, as heck. And that was one thing that, Neil Bridges, he's a, a good guy, met him at Black Hat two years ago.

And he said, it's really interesting. Everybody's looking at what you're doing. He goes, you bought the, you brought the pew pew factor. To cyber security. We never had that before. It's always been boring, right? And so that's actually one of the things we're looking at is when you do the games, you actually have a whole visual of the network behind you.

So you can actually see when somebody moves from box to box, you can see there's a nice sound effects and everything else, and you can tell what's going on and you can watch that. We don't have a Player versus player version yet, even though we're working on that. But certainly the ability to go in there and watch on a screen somebody actually going through the game and watching them advance through the network.

You know, you unlock a box and all of a sudden, you know, it's you know, it's got a key unlocking and it goes above it. And so you've got all the video game features that make this suddenly more interesting while still keeping it technically very accurate. That was one of our criteria, we had in the beginning.[00:37:00]

I just did a presentation on this for an ISIS cyber security group focused on increasing diversity in cyber security. And I said, so you go to game based training and all of a sudden everybody in your dev team is like, Hey, we're building a video game. And, you know, then you've got, you know, It's somebody building an orc swinging a sword and that was one of our rules.

I said, we don't have any orc swinging swords here, right? Every single command we have has to be an actual real world command. It may not be full capability. Like if we do Nmap, it may not have every switch that is available on the latest version of Nmap, but it's certainly going to have all the basic switches and every switch it has is going to have their same exact functionality.

So we're teaching exact skills so that you can get people in there. And everything they do is actually something they're going to be using on the keyboard. You get very technical people in there and when they know how to actually use all these tools, you know, they can actually start flying and doing some real world challenges with them.

[00:37:50] **G Mark Hardy:** You can remember that. So I'm not going to try the Orc++ sword command. It's probably

not going to work. But the thing I came up with where we're talking a little bit earlier, I wanted to mention is this concept of retention. [00:38:00] And what do I mean by that?

We find out as in this, as managers and as bosses in the cybersecurity world, there's a almost negative unemployment out there for good people.

It's very difficult to hold on to your best people. And there's always somebody to offer a little bit more money or a little bit something or else. And yet. In some cases, we can get people to stay for long periods of time. This is a big challenge, particularly for the military and government, even a nonprofit that can't go ahead and write bigger and bigger checks.

But what I find is this is I remember a study I read a few years back and I'm trying to remember the source of it because I like to cite sources when I put

something in there. But John Pescatoria told me about it and he said that the number one thing that kept People in their cybersecurity jobs was not more money.

It was the willingness of the organization to invest in their training. And specifically the fungible coin in that realm is certifications. And yet what we find though, is that if you want your people to stick around. It's how they feel like they've been treated. [00:39:00] Yeah, you get to a certain level where you've satisfied, you can provide food and clothing and lodging and shelter and Maslow's hierarchy.

Okay, great. You're not going to starve and you don't have to walk to work backwards in the snow, uphill all winter long and barefoot. But beyond that point. Do you see the ability to utilize a game based training scenario on a more regular basis to create a sense of camaraderie much like as you get into the, like the Duolingo and you're thinking about, well, the person who, you know, been there for two years, I've only been at it for six weeks now, but I haven't missed a day.

And so the point is, is that you get going, but can you create that sort of a camaraderie where if someone else comes along and they said, well, Hey, we'll give you more money, kid. Well, what do you guys do? Well, we work a lot. Well, we work a lot too. What else do you do? Well, you know, you can punch the pubs at night.

Well, we get to go ahead and do game based learning. This is pretty cool. You guys don't have that. Nah, maybe not. So, I don't know if that's ever come up, but [00:40:00] to me, that's what struck me from a management perspective is that I can see this as a key retention tool and easily worth the price of investing in it if it creates as more of a sticky, Nate, you know, people want to stay with you.

Have you seen that from your client base or if not, well, here's an idea. You can go ahead and push that.

[00:40:16] **Eric Basu:** absolutely. One of our clients is a huge healthcare company and he actually, interesting, a younger guy, maybe in his mid forties, and he said, I don't play video games, but my cybersecurity people, it's like their golf. He goes, I need this to attract and retain the best people. and my last company, Sentek, I actually found, I would say this all the time, I get a 10x return from educating my employees. Yeah, they could potentially take the certification and go somewhere else for more money, but I generally found that

wasn't the case because they knew that they would be able to stay and get more education.

And that was from down the low levels where they're getting PMPs to the executive level where they're going to Harvard negotiation courses. So, absolutely, I've seen that as a reason for CISOs to buy the product. I had another CISO say that, he has an Immersive Labs. And Immersive [00:41:00] Labs is, you know, 100, $300, 000, you know, digital twin of his network that people can go in and anytime go practice their cybersecurity skills on a copy of the network.

He said nobody ever uses it. It's boring. Nobody wants to do it. You know, he can run mandatory capture the flags and, and exercises in it, but he has to actually do that in order to get them to do that. And so, that's the advantage of the game based learning. You have something that people want to do, and they want to do it for a variety of reasons.

One, it's fun. Two is that you're right. The competitiveness against their, you know, that's one of our customers. We send a weekly email out. We give them a different challenge. Hey. Here's the challenge for this week. And then the next week we show them how everybody did in that challenge. Now maybe they, you know, they, you know, some did well, some didn't.

This serves a couple purposes. One is it increases the camaraderie and the teamwork aspect of it, right? Two is it shows the CISO which one of my people are best at these things. Like everybody wants to go offensive cyber security, right? I want to be a pen tester. Everybody wants to do that. But it turns out one of his best people at [00:42:00] pen testing who can beat some of his engineers with 10 years of experience is a relatively junior person who has no technical degree.

Right. And, so we found this also, we just did an event in Hawaii with the high schools and colleges in Hawaii, the winner of our competition, our CTF competition. was a young girl who, not young girl, she was in college, young girl, I guess, but, who had, she did not have a technical degree, I forgot what her degree, and I want to say liberal arts, it was a liberal arts degree, but she beat everybody.

She beat all these other people, her computer science majors and math majors, and the CTF. And so, coming back to your point is that.

this is a great way for organizations to, I mean, hit a number of different things, camaraderie, team building, overall engagement, continuous learning, and from the CISO's perspective, you get to look on the back end at all the metrics.

You're not just relying on anecdotes where somebody's talking about it at the water cooler, or in an online chat of, hey, I did this. You can actually look at the metrics in the back end and go, man, she's really, really good at this. Let me go ahead and look at trying to maybe give her [00:43:00] some training to move her over to this.

[00:43:02] **G Mark Hardy:** Wow. So, yeah, there's, we've covered an awful lot of ground here and, we're almost at the 45 minute point. So let's, let's kind of recap a little bit. So we talked about the concept, the difference between game based learning and gamification. And that was my first term and it is incorrect, but on the game based learning, what you're doing is you're taking some subject or whatever, but you're, you're putting it in the context of some sort of an interactive environment, which.

People tend to get into the flow, and everybody remembers Sixth Sense Mahaly's book on flow and his work. I understand exactly what you're meaning there. And so as a result, they will learn without even realizing they're learning. The example you gave was somebody being able to say, hey, wow, I know all these Linux commands because that's how I used it to go ahead and, well, rescue the princess or whatever it happens to be.

Second. That I think is an important element is that it will work both as a technical level for people who are used to video games, but could also be applied even at the board level, because it's got the flexibility that you're not going to have [00:44:00] goofy characters and things like that. But it's going to be scenario based with such that board members or different executives could see themselves in these particular roles and say, yeah, that makes sense.

You know, we had, Andy, an opportunity to talk a little bit about some of the fiduciary. Issues that come out both with boards and CISOs. And as a CISO, you need to know kind of where that limit is in terms of, yes, it has to report this to the boss. And then if it's going up to the board, the importance of being able to communicate, not in technical language, but in board language.

And then from that point, what we want to be able to do going forward is ensure that we have some sort of stops in there. So if we say, Hey, there's a real problem and they're not getting it as a CISO, you need to be able to know how to kind of ratchet up the heat and things such as that. Is there anything else that I

didn't cover in the summary that you'd like to make sure that you'd share with our audience before we wrap up?

[00:44:50] **Eric Basu:** No, that's a great summary. Great notes. I agree with you. You hit it all.

[00:44:55] **G Mark Hardy:** All right. So I do want to thank you. So Eric Basu, the founder of Haiku. [00:45:00] Which, look, if somebody wants to find out more information, where do they go? Which, what's your website?

[00:45:04] **Eric Basu:** https://www.haikuinc.io/

[00:45:09] **G Mark Hardy:** io. Okay. Have you ever been to io? Seriously, there is a place. It's a, it's the British Indian Ocean territories. It's known as the footprint of freedom. It's Diego Garcia. It's a thousand miles south of the tip of India. And as a Navy guy, I have been there more than once back during Operations in that part of the world.

[00:45:32] **Eric Basu:** I just learned two or three new things. I've never been to Diego Garcia though.

[00:45:36] **G Mark Hardy:** You're not missing much. Okay. For everybody out there, thank you very much for tuning in to CISO Tradecraft Podcast. We hope that you found this of value to you. We're talking about the importance of game based learning, how we can use that to both educate people, attract and retain people as a result of having something that's interesting, build a camaraderie, meet not only compliance requirements, but be able to address unique organizational [00:46:00] requirements and up to and including getting to the board of directors. So until next time, this is your host, G Mark Hardy. Thank you very much for listening or watching CISO Tradecraft. Until then stay safe out there.