2024-08-26--t08-26-31pm--guest258042--deb

Introduction and Welcome Back

#End Intro

[00:00:00]

[00:00:00] **G Mark Hardy:** Well, 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 am here with a former guest, and now I'm excited to have her back, Deb Radcliff, whom we talked with back in May of 2022.

And that was episode number 80, for those of you who are keeping track. But Deb, it's great to have you back on the show. Welcome to CISO Tradecraft.

[00:00:40] **Deb Radcliff:** Thanks! Super good to be back with you, and also nice seeing you at Black Hat this year, too.

[00:00:45] **G Mark Hardy:** It was, so we're not that far from Black Hat. So there's still a lot of people that are going through all the leftovers, little bags of tchotchkes that they brought home, if you're an attendee, or if you were one of the people who happened to be there and [00:01:00] was. Yep, you got all that. And you were an exhibitor, then of course you got all your list of all of your people that you picked up and things such as that.

And so the point is, is that what have we got as a result of that, hopefully something that's actionable, that'll help people out with their jobs and their careers and things such as that.

[00:01:17] **Deb Radcliff:** Amen.

Black Hat and Security Leaders Dinner

[00:01:18] **Deb Radcliff:** Yeah, at Black Hat, it was an interesting show for me because I, most of my show was before the show. So there was this amazing security leaders dinner hosted by the Wilkinsons. They're funding and they have a couple of startup companies in cybersecurity and I couldn't believe all the movers and shakers that were there.

That was Monday night when the Briefings actually started on Wednesday. So my big events were actually more things like that this year than the actual show floor. What about you?

[00:01:48] **G Mark Hardy:** Well, I somehow didn't make the cut for the security leaders thing. So I want to, and maybe other people didn't. So first of all, tell me about it and then B, how do you, how do you get on that short list there in Vegas, baby, to go ahead and do [00:02:00] something cool like that?

[00:02:01] **Deb Radcliff:** Well, I know that Wilkinson's through Alyssa Knight, who produces videos and shows around cyber crime. She actually takes original FBI cases and converts them into actual, it's almost like a cyber FBI show. And she, her next series is actually going to go on HBO, so she's been graduating from her own platform.

that she produces on NightTV. com. So I've known Alyssa since she first started producing. I went to one of their shows that they did in a theater in Las Vegas, especially just for her to see the show. There's a lot of excitement. The actors were there signing posters. It was like real movie stuff. I wouldn't say it was the highest, highest quality, but it was pretty close.

And she's doing these on a budget and she's got, uh, The Wilkinsons have been sponsoring and funding some of their shows and so I met them all [00:03:00] there and I couldn't believe I brought Renee Gutmann with me. She's a CISO who used to be at Coca Cola and Time Warner in the beginning and, and, uh, Caribbean Cruises and Campbell Soup and she and I were pretty excited.

There was just a lot of hubbub and I thought, well, this is exactly sort of what I'm trying to do with my cyber thriller books, which is to get them onto like Netflix. So. It was just a really nice meeting them and they really know a lot of people. The, the restaurant was packed. The dinner took like three and a half hours because it was traditional Italian.

[00:03:33] **G Mark Hardy:** Oh yeah, that's what I'm thinking.

[00:03:36] **Deb Radcliff:** I just kept getting up and moseying around and talking to other people. And, you know, there were reseller companies there, but mostly they were all straight on. The CISO of Wynn Resorts was there. And I actually went to a SBOM meeting, Software Bills and Material meeting, on Tuesday, at the Wynn, the next day.

So there's a lot of little coincidences like that. [00:04:00] So, it was really nice. They had great mocktails too, since I don't drink. So, they had like a world class bartender. And she made me some good fruit drinks instead.

[00:04:11] **G Mark Hardy:** Well, that sounds great. So Monday night at the security leaders. So maybe put that on my list for next year, if I can somehow add some value to that, because a lot of us see these special events that take place, but you wonder, you've got to get invited to them.

[00:04:25] **Deb Radcliff:** Well, remind me and I'll try to get you invited next year. My memory isn't what it used to be, so I need help with that.

[00:04:31] **G Mark Hardy:** that's no worries. Now, who are you again?

[00:04:33] **Deb Radcliff:** Uh,

[00:04:35] **G Mark Hardy:** That's contagious. So, yeah.

The Evolution of Cybersecurity Conferences

[00:04:39] **G Mark Hardy:** So a couple of events that I went to at Black Hat, they had some evening receptions and things such as that. One of them over at the, um, the Irish place where we get together and you could get together for that. I think, uh, what else did they have?

A couple of dinners, more light appetizers and sit down dinners. I think last year I did a little bit better. They [00:05:00] had some really nice one where you went to some resort and you went Place inside a place and they had sit down, they rolled cigars for you and things such as that. And so there's a lot of activity out there on black hat.

And so I kind of wonder, because I used to go to. RSA. And I, last time I went to RSA, I spoke there and I don't know if I got my ROI. That is to say, even though it was a speaker, you didn't have to buy a badge, you still gotta pay for

the airfare, you gotta pay a ridiculous amount of money for the hotel, the meals, and things such as that.

Do you think that Blackhat is becoming like RSA where people just go for the parties and for the contacts, or are they still going there for the talks?

[00:05:39] **Deb Radcliff:** They have been, they still have better talks than RSA. That talks also translate over to DEF CON, which I know you also went to. I feel like I'm getting way too old to spend that much time in Vegas anymore, but I used to do the whole circuit when Black Hat was small and DEF CON was over at, what was the name of that hotel where they threw the chairs in the pool?

And, [00:06:00] um, it was off

[00:06:01] **G Mark Hardy:** you like, are you talking about the Alexis Park?

[00:06:03] **Deb Radcliff:** the Alexis Park and they had a big tent out back with air, you know, misting and air conditioning and spot the feds contest and all of that. I heard of this year it was at the convention center. I heard from hackers that they were kicked out of the hotels they usually use because for the show because Caesars got kicked out.

Uh, Ransomware a year ago, or in the last year, and everybody thinks the hackers did it. I have tried my whole career to try to distinguish between criminals and hackers, but it's hard when a big company like Caesars can't understand that the hackers are the researchers, who are actually ultimately going to help protect them.

by discovering things and then making that discovery public. So people can work on workarounds and fixes and replacements. And I just couldn't believe that this happened. And a bunch of people complained about the venue. Some thought it was great because it was [00:07:00] bigger and more professional. Others thought it was too expensive.

It was, you know, the food sucked and you were limited to what they had at the convention center. You couldn't bring anything in. So I'm not sure how that went, but it feels like all of that has gotten too big. And like B Sides now is the place to go.

[00:07:19] **G Mark Hardy:** Yeah. And for those who don't remember the origin of B Sides, I think it was back at DEFCON 12 when all the senior speakers, in fact, my talk got turned down that year because, well, you've spoken before.

And a lot of people have said, well, we want to have everybody new. And that was kind of our Hacker Jeopardy trivia question, which is the one of all those DEF CONs that we didn't have Hacker Jeopardy.

It was DEF CON 1 and DEF CON 12 when they tried out something different and it kind of bopped. And so we brought back regular speakers and things like that. But the genesis for BSides was born. Now you and I are old enough to remember what BSides actually stands for. And I think a lot of people today have no clue what a B side of a 45 record was.

[00:07:56] **Deb Radcliff:** Oh gosh, actually I couldn't, I didn't know what it stood for, [00:08:00] so

[00:08:00] **G Mark Hardy:** Because when you got a 45, because you normally get an LP of 33 and a third, you get those Columbia records, 13 albums for one penny, you taped a penny to a postcard and you dropped it in the mail. This is back in the 70s. And you got a 45 that would have a single. But on the back of the single, because it's something that everybody wanted, you'd have to put something on the, from the A side, the B side and the B side was also ran music, but sometimes if you got a really good double sided 45, you got a hit on both sides because the B side record.

Publishers didn't expect to be great, turned out to be really good. And then you got double your money worth for that, uh, 45. So the idea of a B side was ideally something that you didn't originally show up for that turns out to be really great. And in fact, that's what B side happened is a sidecar, so to speak, to an event like DEF CON.

And then it has come into its own right over 1000 B sides

[00:08:55] **Deb Radcliff:** Yeah. And they keep them small, and it's all about the size. The [00:09:00] talk, you're in one room for most of the day with different speakers. Now, when I go as a journalist, I get approached by the organizers saying, don't quote anybody without permission, even the speakers. And I'm like, dude, I know, you know, and it's like the old black hat days, right, or the old, uh, Def Con days.

Where the same thing, you know, they were very touchy about having journalists in the space. Normally, B Sides just helps me write better stories for CISOs. It helps me understand what's coming up, what just happened, what they may not be aware of. And so I use B Sides as, you know, It's an idea generation

place for my content, for my articles and video interviews that I also do, uh, around these topics.

And my audience, like yours, is the CISO, especially for my articles that I write for CSO Magazine. But my other audience is the DevSecOps product development side for Embedded Systems for my TalkSecure video interviews that I do. So I'm [00:10:00] Climbed up the ranks and gotten a lot smarter around DevSecOps over the past few years because of this particular column.

And now I'm able to sort of Say, this is where this stuff affects CISOs, and this is where CISOs can affect their product leaders in their companies. So, all comes together, DevSecOps feels to me like DevOps and Engineering and StartLeft, not ShiftLeft, but literally StartLeft, is where we need to be putting our emphasis right now to make it easier on the CISOs and the enterprises they're managing.

At the other side of the spectrum,

[00:10:37] **G Mark Hardy:** Now that's really good insight, particularly because, you know, Talking to you, of course, I've known you for a long time, and you're a career journalist. You're not a career IT security practitioner, so there's no geek about you, and yet you are very credible, and you write well, and you take the time to get to know both your audience as well as your subject matter, and so commend you for that one.

AI and Cybersecurity Trends

[00:10:59] **G Mark Hardy:** [00:11:00] And so, As you interact in that, so when you were at BlackHat and kind of looking at it from a journalist perspective, what is it that you saw as a big trend this year?

[00:11:09] **Deb Radcliff:** AI. Everything. AI. And they forget that we all know what machine learning is. We've been using it for years, but all of a sudden, every security product includes AI and all of a sudden, every security product, forget, protects against AI booboos. The problem is, from the DevSecOps side, I'm not seeing that yet.

The security tools out there that scan code don't know what to look for that can be wrong with an AI system you may be getting ready to install in your organization. Some of the help that I've seen is really coming from places like Salesforce and AWS that's providing the safe buckets for you to run your AI in and the safe data pools and data lakes and it.

isn't actually all that [00:12:00] much different than what organizations are already doing to secure their third party apps. Those are always going to be the quickest to embed new technologies into their apps. So the trend for CISOs is watch out for the hyperbole, watch out for the cloak and dagger stuff that isn't real.

If you're not using the kind of AI that's been jailbroken, You're in a much better position if you're not using the AI platform itself, but you pulled the, you pulled it into your organization as opposed to giving everything, all of your trade secrets away at a browser based application. You've got a better chance of using AI to your, uh, business benefit.

And that's the way I see it. And all these tools coming in safe AI, yeah, there are things that AI will do. uh, in the large language models, especially that can bring, you know, open the door to new types of vulnerabilities. So now [00:13:00] we've got to adjust our firewalls and other technologies that don't know how to look for common language, English language breaches.

And when you go to a black hat and RSA, you really don't see it that simply. They make it a lot more complex than it really has to be.

[00:13:19] **G Mark Hardy:** Interesting. Yeah, one of the companies I talked to there, they were in the startup area. One thing I like about BlackHat is they'll have little areas where you can get companies that are just coming out of the starting gate. And I caught up with Sunil Yu with his Knostic where he is using AI and applying that to be able to effectively interdict how an AI tool can access a corporate data system.

For example, if the CEO says, Hey, Uh, AI, it's trained on my internal data. What's my forecast for next quarter? Well, here, you're the CEO. You should know that. But if Joe over in marketing wants to know that, I said, well, Joe, it's nice that you want to know that, but you really don't need to know that at this [00:14:00] particular point.

So it's a way to interdict that rather than try to do the traditional DLP data loss prevention. And Sunil, by the way, won the award for the best new data loss prevention. Company there, and that's a great thing. And he was one of my advisors 10 years ago when I was doing my startup, CardKill.

[00:14:16] **Deb Radcliff:** Awesome. Uh

[00:14:17] **G Mark Hardy:** Another company I saw, Level 6 Cybersecurity.

They have gone ahead and they have the Level 6 InfoSec Strategy Network. And it's an AI powered type of a tool to make, Business intelligence and come up with a cyber security strategy. And I think a lot of cyber security experts would say, well, I've got some sort of a strategy, but maybe it's something that either I kind of cobbled together.

I inherited or some consultant. Okay, I'm a consultant. I do that is come and write that and they're looking at ways to mobilize that. So a lot of brilliant ideas that are coming out of there. Uh, and so. One of the things also that we've looked at with AI and something that is actually getting into, almost into the warfare and the kinetic stuff.

We were talking a little bit about this [00:15:00] before the show is AI and drones. So that's an area that I think of you're of interest. And so,

[00:15:08] **Deb Radcliff:** So in my cyber thriller books, and I should have brought my books out to show them to you. Great, great. That's the first one. Thank you, G Mark. He's got all three of them. I still owe you autographs. That's first book, second book, and third book.

[00:15:21] **G Mark Hardy:** book three, and we'll put the links in the show to Amazon. Go ahead and get yourself a good hard cubby. They're awesome reading, by the way. I know we covered the first book. in their first episode a couple of years ago. And you were talking then about, I'm going to fill out the books, but you've got them, they're, they're published and they're out here and they're awesome.

[00:15:38] **Deb Radcliff:** I know I wrote three books during COVID. Well, two, the first one was already done when COVID started, but I have this big lanai here in Maui and I was just sitting out there writing my books. It was work though, there's a lot of research, there's a lot of fact checking, a lot of people like you had to fact check for me before they published, especially around my military stuff because I've never been in the military, you [00:16:00] know, and all of that.

I should have been, I always wanted to be. And thank you for your service, G Mark.

[00:16:05] **G Mark Hardy:** Appreciate that.

[00:16:06] **Deb Radcliff:** Yeah, I appreciate that. We appreciate that. So, the point in book one was the overreach of technology. Globecom breaks the world,

uh, takes over the world with human chip implants. We talked about that in the first one. Hackers raise up to break its network backbones.

Now, to me, hackers are the good guys. I've hung out with the greyhats. And the white hats and some of the gray hats who try to act scarier than they really are, you know. But, and then I wouldn't even call black hats like, I don't know if I'd call them hackers or not. Because if you're a criminal, you're a criminal.

And if you're a hacker, you're a hacker. And that's the way I've always seen it. And that's the way I've always written it. In my books. I wanted the world to see what hackers are actually doing for the world. I wanted them to see what CISOs are up against. And I wanted them to see what developers were up against.

And I was able to pull all that through on these exciting, [00:17:00] fast moving drone war scenes and, you know, book one starts with a kamikaze drone and it published a year before the Ukraine war. No one really talked to me about whether these things existed or not, but I Extrapolate, it seemed possible you could arm some of these with some explosives and slam them into a wall and blow up the wall, which is exactly what they did in chapter one.

So, we moved, you know, so the kinetic warfare, and that's the whole thing too, I've done some work around, what's the difference between cybo cyberwar, information war, And I forget what the third one was, um, Cyberwar, Infowar, and Cyberwarfare, I think is what I called it. So we have attacks on the infrastructure happening in Book 3.

We have hackers helping the NSA. Undo the damage, get the keys to decrypt some ransomware at the system operators. Mark Sachs, you know him, [00:18:00] he really had to help me with how those hacked works. You know, they not just, they use the ransomware to befuddle the system operators while they had other malware going all the way out through the controllers and they were being remotely controlled.

And that's

[00:18:16] **G Mark Hardy:** misdirection. Any magician will tell you about that. Hey, look over here when the action's going on over here.

[00:18:21] **Deb Radcliff:** Yeah, because Mark said you can't have ransomware actually shut down the power. You can shut down all of the, like the California independent system operator systems, but those aren't the ones that are actually

running the, at the power plants. And so you need a secondary attack to go through and get all the way out to the power plants.

And that's how I managed that. So the hackers helped be, you know, Find the decryption keys and stuff in book three. And so we've got the, all the different forms of warfare are covered in all three of my books. And I did it with some strong characters, a female [00:19:00] lead named Cy, short for Cyanthia, formerly Cindy Frank, a forensics investigator for DOD.

Very good at her job, by the way. And then we've got some people who actually do like guns. And so that would be Desolation. He's former, uh, Navy and former, we really don't know what military branch he was at, but he was highly functional, good shot, you know, meticulous about, he loved his drones and bombs and things like that too.

He made his own weapons. And then we had a lady named Allure who liked guns too and got better and better and became Cy's protector by book three. So we have all different elements going there, but the CISOs themselves. are getting shot down in book one because once Globecom's backbone is broken there's competition for who's going to pick up the pieces and there were four global CISOs and three of them were, well two of them were shot down, one of them got away [00:20:00] and of course the CISO from secretly from Russia, um, didn't get involved in that because we have to have some protagonists, you know, and so anyway, and then in book, uh, two, they had stolen, the hackers had stolen artificial intelligence that was under development in a Russian work camp, and they released and freed the developers, got them to France to finish the AI, and, They come under the gun.

So, there's an attack on their development center, and it's drone induced, and finally the bad guy gets his comeuppance, and so, I just had to try to put all this together, but how do you do it so that people will actually enjoy reading it and not be bored like they're reading a textbook?

[00:20:50] **G Mark Hardy:** Yeah, so is your idea about getting, uh, Pavel Durov to go from Russia to France to get arrested?

[00:20:56] **Deb Radcliff:** yeah, that! I, that was all

[00:20:58] **G Mark Hardy:** I mean, you're telling me these things and I'm [00:21:00] thinking like, that's in the news today and things such as that.

[00:21:04] **Deb Radcliff:** And that was the thing. Everything I wrote I thought was going to be 10, 15, 20 years in the future. The only thing that might be more futuristic are the human chip implants. We'll see how long that takes. But we've got Musk having a lot of fun with those

[00:21:16] **G Mark Hardy:** yeah, they're already doing that with Elon Musk and things such as that. And it's interesting as you, as you look at this. So what is it like to be able to say, I want to write a book? No. I'm under pressure from my buddy. He said, G Mark, you're like, you're the last guy of your generation not to have a book out.

And I wanted something to be evergreen. I didn't want to have Windows 95 secrets by G Mark Hardy. It just sort of, but, but yours then is rather timeless in a way. And so how do you go for the process? And of course you're a professional journalist. So maybe writing is a lot easier for you of, I got a concept to, I've got a deliverable and it actually works.

And, and how tough is that? And how do you blend that in with the rest of your life?

[00:21:55] **Deb Radcliff:** Well, let me tell you, it took me 20 years to get the first book out of my brain [00:22:00] and onto paper.

The Chip Dilemma: Parenting in a Monitored Society

[00:22:01] **Deb Radcliff:** That was after I heard Scott McNeely, Sun Microsystems, saying, I can chip my dog. Why can't I put chips in my children to keep them safe and know where they are at all times? And I came home and I said to my kids, What would you do if mommy put a chip in you to make sure that you were safe at all times?

My youngest one was eight, my oldest one was 13, and all three of them were like, I cut it out of my body! And I go, great, I've trained them right, you know, so that got me thinking, and then I started thinking of characters! Like, well, you know, If they're going to live, I knew they were going to be in a monitored society.

I knew drones were going to be doing the monitoring. Everything overhead had to be blocked somehow. They were going to have to install their own signal towers. But if they want to do any farming or any chickens or anything outside,

and then I thought, well, mostly they're going to be in a cave and I thought people are never going to read this because who lives in a cave and,

[00:22:59] **G Mark Hardy:** [00:23:00] doesn't transmit very well through a rock anyway.

[00:23:02] **Deb Radcliff:** Right, and I, and I went looking around going, well, a lot of people live in caves, like, there's some designer caves out there.

Crafting Characters: Inspirations and Transformations

[00:23:09] **Deb Radcliff:** So, I started with that, and just sort of kept growing, but like, Cy, Cindy Frank, was a name of a friend of mine who passed, that was her, her civilian name, that was her name when she worked at the Defense Forensics Labs, that was to honor her, but then, she converted into a den mom of a hacker clan, and, and, In the Blue Ridge Mountains.

Okay, so, what's a good name? Cyanthea, sort of like Cindy, and Cy for short, and now she really is Cy. Like, she becomes the character as you work on her. Uh, Allure became Allure. She got more and more edgy as time went on. And Maine is based on Del Chai, who's still out here and still doing, you know, Handicap services for Def Con and things like that.

I think you know him, AP Jelchai. He also wrote his own, um, [00:24:00] Omniverse. illustrated, uh, books. Really good, by the way, if you guys haven't gone, uh, gotten any of them, you should. If you don't, if you want to learn about the goth scene, that's what he was really tied into. So he always reminded me of a lion, so big hair.

So I called him Mane, M A N E. Now, he read the book before it published and he was fine with it, and he's kind of immortalized through it. And there's a couple of other folks in our world, Jim Christie, Chris James. Okay, DOD Forensics Labs, Michael Jacobs, NSA CIO, Jacob Michaels. So I, some of them I didn't even bother to change their names much.

But I stuck to personalities that I knew. Maine is very sardonic, so is Del Chai. Uh, Allure, I just saw across the room, this tall, skinny lady. Friend of Maine's, friend of Del Chai's. And when I made her a warrior, I checked with, uh, And he said, Oh yeah, that sounds like her. Her real hacker handle is Kitty and I started cracking up.

I [00:25:00] sent him a book and addressed it to Kitty and signed it and he gave it to

[00:25:04] **G Mark Hardy:** work, shitty, right?

[00:25:06] **Deb Radcliff:** right. So it's all about at, you have to add a character arc through every story and you have to make people sympathize and believe in these characters. That first book I kept feeling like no one's going to, you know, Like my characters, no one's gonna like my locations, everybody loves my locations, and my characters!

And I have a producer who says I can set a scene like nobody's business, and he wants me to co produce when we finally get past the pre production stage, but he's kinda quiet right now, so I'm not sure where he is, but I know he's working on another project. Uh, miniseries for Netflix right now. So we'll see if this happens in my lifetime or not, but hey, producers, I can still get another producer.

I have not signed a contract with my existing one. Just saying.

Writing Process: From Drafts to Details

[00:25:58] **G Mark Hardy:** And one of the things that I've found in the [00:26:00] writing, now maybe I've been writing too many technical documents for so many years, Or too many CISO Tradecraft podcasts, or you try to be, um, Deliberate about things, or even that in the military. But I just kind of picked a page at random out of your book, and I'm going to read just two little paragraphs, and I'm going to say, how do you come up with this level of detail?

Leonard anxiously paced his penthouse suite at the Watergate Hotel, pausing intermittently to look out the picture window at a wide view of the Potomac River before resuming his pacing again. Absently, he scratched his left forearm above his wrist where his implant itched and when he heard the expected knock at his door he shut a silver colored clamshell carry case on the coffee table and excitedly hurried to the door.

Okay, I'm

[00:26:43] **Deb Radcliff:** Oh, wait, you have to read the next part where they make out.

[00:26:47] **G Mark Hardy:** I just closed the book. I have to go look for it. They want to figure out how they make out. You got to read the book. Go buy, go buy the book.

[00:26:54] **Deb Radcliff:** Sorry you guys, but this is a full spectrum book. There's family, there's sex, there's everything.

[00:26:59] **G Mark Hardy:** [00:27:00] Yeah. But that level of

[00:27:01] **Deb Radcliff:** it's classy.

[00:27:03] **G Mark Hardy:** I've been in a silver colored clam shell thing. Like I say, where does that come from? I mean, it's just creativity. You have to go ahead and sit back and go like, okay, I'm going to come up with 12 adjectives and now you feel like ChatGPT cause you're describing things in extensive detail, or is it just sort of a right brain thing?

That some of us, the left brain people just don't have access to on a regular basis.

[00:27:23] **Deb Radcliff:** Well, I'd say the latter, but also you locations, you know, I've been to the Watergate, I've stayed there. I've eaten in that outside restaurant along the river on the backside of the hotel. So it helps. That's why book. Three was a little harder because I had scenes in China and scenes in France, and thank God for Google Maps now, and thank God for Street View, and all those other things, because I haven't been to any of those locations, but I've been in the Blue Ridge Mountains, and I've been in the, uh, Russian River area extensively, where they moved their camp to at the end of Book One, and where their camp is for Book Two and Book Three.

[00:28:00] So, start with locations you know. The question is, how much description do you give? Some books they way over describe, some books under describe. Mine's fast moving, so I try to make sure that those description scenes don't distract from the story, but I also want to put you in the room with, you know, Dark Angel, aka Leonard Smith, who is a double, you know, he's got the chip, he's working for China Telecom, he's now a CISO over there for Globecom, and he has to hack his own chip, to go have his affair with Psy, and he's the father of Psy's firstborn child, and blah blah blah.

So, all of the detail comes as you're thinking about it, you're writing about it, and you're thinking, okay, so what does the hotel room look like? Oh, remember, there's big plate glass windows that look out over the river. He's

going to be in the penthouse, which isn't very high in the, uh, Watergate because I think it has like seven floors and he's gonna be over there looking and he's gonna have a [00:29:00] special room and he's gonna have the hotel system hacked so that no one really knows what he's doing there because he's hiding his activities and so you, it just starts to come and outline part of it but a lot of times you don't stick to the outline or while you're writing one paragraph and you're thinking two paragraphs ahead you write two sentences below that paragraph so you know what's gonna go next and It's a lot of that.

And then of course it's a lot of proofreading and editing and changing and fixing, it's a book writing, getting the first draft down is huge. Getting it finished is even huger.

[00:29:35] **G Mark Hardy:** I would think there'd be a big, long, steady pull. And of course you have editors out there and for nonprofessional journalists who write something, they said, you know, people I've talked to said the hardest thing is when you turn your manuscript, they go, okay, fine. Get rid of 75 pages. It's like, but I wouldn't have written 375 pages if I didn't think it was good.

I said, I know that it was Mark, Mark Twain, who had said years ago, he said, if I had had more time, I'd have written you a shorter letter. And [00:30:00] so they're There is value in brevity up to a point in so far as, as you were saying, you get rid of the excess fluff and things that don't really contribute to the character development or the flow of the plot.

It may be just superfluous or sometimes you get books that are just padded out the yin yang with information because they got to get to some minimum page count and they're not there yet so they just throw junk at it. And so I think for people thinking that they want to write a book, first of all have to figure out what type of writer are you.

Are you a minimalist writer and you're going to have to add stuff or do you tend to write too much and then you refine it down and like any refining you end up with a pure form of what you're looking for at the end.

[00:30:41] **Deb Radcliff:** One of my biggest editors for that, honestly, was Mark Sachs. So, when he was reviewing, he's, uh, with McCleary Research Institute for Critical Infrastructure. He's former White House, uh, Cyber Security Czar, or whatever his title was. Former military like you. And he would say stuff like, [00:31:00] So, little, tiny blurbs, like, said the television announcer, comma, a transgender person with purple hair, he goes, just take that last part out.

We don't need that. You know, it's really about the people watching the television monitor, not the people on the television. So I fixed like a hundred places like that when, and even though it was only taking out seven, 10 different words, it was distracting to leave them in. And so I listened to him and I went back and.

When I edit it, I edit out a lot of that stuff, and I think it kept the flow going better, like he said, and yeah,

[00:31:38] **G Mark Hardy:** Yeah, so that's great.

Future of Cybersecurity: Autonomous Systems and Legal Challenges

[00:31:38] **G Mark Hardy:** So you start out in book one, as you had mentioned, about armed drones and that predated the conflict over there in Ukraine and Russia, but now here we are into the third year of that. And it still continues. And so what tying a little bit of fiction to real world, what are [00:32:00] we seeing changing out there for you as a journalist, you expose yourself to a lot of information and what that role is going to be different for people in cybersecurity, because all of a sudden now, between a lot of the infrastructure hacks, not the kinetic stuff flying a drone and blowing something up, but being able to break into or alter, or change the production system in OT.

And a lot of people don't realize that the controls we have in IT, information technology, are not well reproduced in operational technology. And this is a little bit like the 1990s all over again, where you have a hard, crunchy shell with a soft, chewy center to go ahead and, uh, use the Bill Cheswick description

[00:32:40] **Deb Radcliff:** the old description, we've heard that for decades, yeah, um, so, I remember writing an article, Computer World, I don't know, it could have been 20 years ago, about automated, uh, weapon systems in like the lobby of a [00:33:00] high security business and who's going to pull the trigger on that? Will it be? Automatically be doing that down the road, and this is now where we're in the era of AI.

So I was writing sort of like, you got the camera systems in an unmanned lobby, someone's coming in with bad intentions, the system's able to figure that out, you've got weapons and turrets up there with the cameras. So who pulls the trigger on that? And I pictured it being automated completely. I wasn't thinking

AI at the time, but I was saying, you know, who controls this technology and who makes sure that it is accurate and now we're the drones.

I mean, how are they producing so many drones so fast? That's my first question for what's happening in Ukraine and Russia. And then those drones are still being. flown by human beings. And in my book, they're still being flown by [00:34:00] human beings, but the military, the U. S. military, and I know the Chinese military, um, organizations are really fighting for autonomous.

Warfighting machines like drones, which means you see those in the horrific dystopian science fiction where you've got a canine bot just firing at people and no one's controlling it, for example. Right, and the Terminator, and I used to say, oh, we're nowhere near the Terminator, but things are moving so fast now.

It's really scary because it, even if the machines don't say, we're going to take over the world. Okay. How do you guarantee accuracy if a machine is literally firing something at a human being? If they're causing harm to humans and everyone's like, oh, there's this law, they won't be able to, bullshit, excuse my language.

But as I'm watching what's happening in Ukraine, all I can say is at least there's still [00:35:00] humans operating. Those drones, uh, but again, how are they getting so many drones so fast? Because they're getting shot down and they're sending like armies of drones out.

[00:35:09] **G Mark Hardy:** And because they're cheaply replaceable, you take a look at the sophistication, of course you look at the supply chains, and we know what countries are developing and then exporting those over to Russia, and I'm not going to get into that detail, uh, but the thing is, you did mention something interesting about the autonomous systems, and let's compare our drive, our record with autonomous driving vehicles, and we have some, had some situations where Some unpredictable events have taken place, like a

[00:35:34] **Deb Radcliff:** A comb.

[00:35:35] **G Mark Hardy:** with nothing on it cutting across the road, and well, okay, I can see the horizon.

I can see the road. I can see the dotted lines. I guess I'll keep going. Oh, bad idea. And a lot of these things aren't the fact that the, we have malicious programmers or that the software doesn't act as intended. It's just, we never thought of that. These are boundary conditions that take place. And like my

friends who are commercial airline pilots, they say, Our jobs are [00:36:00] hours and hours of sheer boredom interspersed with moments of sheer terror.

You're there for when something doesn't go right, and 99 percent of the time you could be just fine, but that 1 percent could be the difference between life and death for everybody on board, and that's where you go ahead and you do your kung fu and make things happen. So as we look At the shift of responsibility from human operators doing human activities, to human operators programming computers to do things, to now we have semi autonomous devices that are still run by humans, that last leap to say we're going to let these devices decide on their own is is got to be a real concerning element.

Now, there's some groups who say we're going to do it anyway. But in a way, you're getting into an area, almost like we talk about chemical or biological or nuclear weapons, a CBN, uh, that we just don't want to go there because it just creates its own Pandora's box. Do we see [00:37:00] autonomous weapons as falling into that as dangerous as chemical, biological, nuclear, or is this just a bridge too far at this point?

[00:37:10] **Deb Radcliff:** Maybe not as dangerous because you could launch a chemical weapon and hit bazillions of people, but my question to you, G Mark Hardy, I'm turning this one on you. Whose responsibility are they technologically? Are the CISOs going to have to oversee these things if it's something that their organization is using, like those security guards at the front door of their business places, for example.

Or the military is using, uh, is it the CISO of the deployed arms services? Who is it that's responsible for this tech?

[00:37:51] **G Mark Hardy:** It's going to be the decision maker who has the Title 10 authorities that is well defined. And as a general, you don't go into warfare [00:38:00] anymore without your lawyer by your side. And if you look at, for example, and I will speak theoretically because I haven't worked there, but you go to NSA and work on the offensive warfare package, you got some consultant from Booz Allen who's keying this whole thing up ready to go.

And then the lieutenant goes over and says, General, please push this enter key. I mean, he looks at the lawyer and said, can I do this? And the lawyer, ba title to end section, da da da, Yes, you may, sir. And off it goes. Because that's the person who can actually launch that cyber package, so to speak. And you want to do it within, the constraints of our legal system, which may differentiate us from some of our national adversaries who don't really care what the book says.

And so in a way, the hand tied behind our back is holding The rulebook. And the rulebook is expressed in public law, which dates back to the Computer Security Fraud and Abuse Act of 1986, as

[00:38:57] **Deb Radcliff:** Oh yeah.

[00:38:58] **G Mark Hardy:** Microsoft [00:39:00] DOS version 3. 1, maybe 3. 1. 1, might have been the standard version of DOS at the time, let alone Windows, let alone everything we have, and we have not seen fit in our country to update that legal basis for making these decisions.

in getting close to 40 years now. And so as a result, going a little bit off topic here, but probably germane to this, we look at recent Supreme Court decisions with respect to, for example, the Chevron doctrine, which had said essentially, if Congress was ambiguous, the federal agencies can make up their minds what should be.

And they said, no, we're going to kick it back and balance those things out and say, Congress, it's your responsibility to be very specific about what you want. And federal agencies, you don't get the chance to invent your own rules and regulations that are outside of the scope of what Congress gave you, which in cybersecurity is going to be very interesting to see how that progresses.

And also, as it seems that our legislators don't seem to be prioritizing cybersecurity as the most important legislation to get [00:40:00] passed, particularly at this point in the election cycle. Thank you. And as a result, we're going to find ourselves in a situation where there's going to be a vacuum out there.

And in that lack of policy, that lack of law, and that lack of precedent is where I think lies the future for some parties, probably United States, not necessarily other cyber combatants out there. In that you're going to have to say, wait a minute, where's my guidance? Well, what does the lawyer say? And the lawyer is going to say.

It depends, and

[00:40:34] **Deb Radcliff:** Uh huh.

[00:40:35] **G Mark Hardy:** answer, and that's not going to, you know, do you launch this thing or not? Do you put your career at risk? Do you put people's lives at risk? And so, I think we've got a lot coming down that's going to make

cyber security very, very interesting. And you say the intersection that we see now between cyber warfare and kinetic warfare, basically, it's called warheads on foreheads, is taking place, ending.

And now what we're going to find out is that the expertise that we develop In our cyber security [00:41:00] careers and the ability to lead and manage that that we develop in our careers becoming CISOs are going to be very relevant to future conflicts and it's not going to be you carry a rucksack eight miles up a hill in combat boats is your qualification, it's do you understand this technology?

Can you make critical decisions? And in a time frame where computers are fighting other computers and decisions are being calculated in milliseconds. There's not time to put a human in the loop. Game over by the time you make a choice. And so, that's semi

[00:41:34] **Deb Radcliff:** who, and then you, and then that falls over into liability. Like what we're seeing with SEC rulings today, your network's insecure. The CISO is liable. Or, in the Joe Sullivan case, you guys blew it, the CISO needs to go to jail. Okay, so we've got a lot of that happening in corporate, traditional enterprise scenarios today.

What 15 [00:42:00] years from now, 10 years from now, things are moving so fast, God knows how soon this will happen. If a, something goes wrong with a device that has weapon capabilities and maybe you're the CISO of an Amazon business who's installed these things at their warehouses to protect workers or an airline, something in the plane, And it's all technological, and it's all something that the CISO should have known about being installed, something they should have known about being safety checked before it went in, compliance, everything else.

Something happens. Who's liable? Are we going to have the CEO or the head of the military turn around and blame their CISOs?

[00:42:46] **G Mark Hardy:** Um, maybe we'll find out. I mean, we're getting close to the end of the show here, so we Let's, let's think about the little things going forward. First of all, what can we expect from Deborah Adcliffe in the next year or two? What do you got in that great mind of yours? What's coming out next? A book four [00:43:00] of your trilogy or?

[00:43:02] **Deb Radcliff:** I did leave book three open just a little bit like there's this Potential maybe there's still a version of the AI out there. Maybe there's not um, but right now it's really about pushing to get this stuff in the Um, movies or

a digital streaming series mostly. And like you G Mark, I'm getting older, so I'm going on a big bucket list trip.

I'm leaving on Thursday. So I'm trying to sort of, I don't know if I'm going to taper out of the industry or what's going to happen in the next few years, but I do know that there's this constant struggle about. When is it time to relax? I mean, I'm literally on Medicare now, right? So I'm getting older. So when is it time to relax and start to accept my reward and slow down living in Maui versus.

Trying to stay relevant, that's the biggest, hardest thing for CISOs too, in our industry, is we get a lot of [00:44:00] FOMO, fear of missing out, we want to stay relevant, we're used to being relevant, we're used to being thought leaders, we're used to people knowing who we are, what happens if that all goes away? And I think that's why a lot of us stay in the industry for as long as we do.

What do you think?

[00:44:18] **G Mark Hardy:** would agree. I determined that I am in what I call a momentum profession. See back in 2004 and five, I went back on active duty for almost 500 days. Start up the Center for Naval Leadership. Created leadership training for about 70,000 sailors. I had a crew of 150 instructors, 72 classrooms, about 10,000 student throughput per year.

Pretty large, uh, program that we created. And basically I started from scratch. We worked with a couple other, uh, navy captains who helped load loaded, but they all said, there's no way this thing's gonna succeed. They all stepped away. And I said, I can't pack all these people into an experimental aircraft, so I will go ahead and be the first commanding officer.

And I did, and we pulled it off. And we actually made [00:45:00] that happen. And so from that perspective, it's one of those things where you say, well, Hey, that was great. And one of these little medals up there is if you knew what to look for, I could point it out to you. But what happened to my speaking career at the time I was doing public speaking, I was making really good money doing that and my consulting and my civilian income dropped 99%. So when I came back from my Navy. experience and back to the company said, Hey, I'm back. And they said, well, G Mark, you're the best presenter we ever had, the best keynote we ever had, but we needed somebody. And so someone else is there and they still got eight months on their contract. And so why don't you call us back then?

And I went around and around and they're all gone. And so what I was told by somebody, it was quite true. And maybe it applies for a lot of us in this career path. It's like Hollywood. The biggest mistake you can make is to let them forget about you. And I made that mistake nearly 20 years ago, and I don't want to repeat it.

[00:45:56] **Deb Radcliff:** Unless you're ready. And I'm trying to get ready for that. [00:46:00] Because it's not so important that I spend the last years of my life trying to kill it versus going swimming in the ocean with the whales and the dolphins.

[00:46:12] **G Mark Hardy:** And that sounds like a pretty good way to end the show. I kind of like that. So thank you very much. Uh, Deb Ratcliffe, you hear you, the author of the Breaking Backbones Trilogy, a career journalist who has done amazing things in your journalistic careers, focusing on information security, cybersecurity, continue to come up with great ideas and contribute to the career.

And to the profession. So thank you very much for everything you've done. And we hope our audience enjoys that again. I'll put the links in our show notes. So you can get your own copy of these books. It's worth it. It's worth the time to read this. I will tell you that I don't do a whole lot of endorsing from here.

And of course you've been a friend for 20 years, but other than that, yeah, I still like the books, uh, for those who are listening out there. If you like CISO Tradecraft, don't forget to follow us on LinkedIn. We have a lot more than just podcasts. Also, we're on most of your favorite podcast channels. If there's one that you are on [00:47:00] that we're not on, let us know.

We'll get there. Watch us on YouTube so you can see me go ahead and wave at you. And otherwise, thank you very much for being part of our audience and listening in. This is your host, G Mark Hardy, and until next time, stay safe out there.