#152 - Speak my Language with (Andrew Chrostowski)

[00:00:00]

[00:00:12] **G Mark Hardy:** Hello, and welcome to another episode of CISO Tradecraft, the podcast that provides you with the information, knowledge, and wisdom to be a more effective cybersecurity leader. My name is G Mark Hardy, and I'm pleased today to have as our guest, Andrew Krostowski. We're going to be talking about digital transformation and the future of work.

Andrew, welcome to the show.

[00:00:33] **Andrew Chrostowski:** Thanks, G Mark. Great to be here.

[00:00:34] **G Mark Hardy:** Well, hey, I'd like to introduce you and talk a little bit about, but first let's put a quick thank you to our sponsor, Risk3Sixty.

If you're tired of juggling SOC 2 and ISO 27001 compliance, you're not alone. The pain points for both are the same. Fragmented audits, endless evidence requests, and mounting costs. But there's a better way. Risk3Sixty offers a harmonized audit process that seamlessly combines both [00:01:00] frameworks. No more duplicated requests or fragmented audits.

Unifying frameworks for mergers and acquisitions. We've got you covered. Contact Risk3Sixty today to learn how to unify, streamline, and create efficiencies in your compliance experience.

[00:01:14] **G Mark Hardy:** Andrew, thank you and glad to have you on the show.

[00:01:18] **Andrew Chrostowski:** Glad to be here.

[00:01:19] **G Mark Hardy:** We've talked a little bit about in the past, you've got kind of a very impressive background, but more importantly, I think who you are is going to be of great interest to our audience.

And this is going to be one of those can't miss shows. So tell me a little bit about your background, please. Some of the stuff that you've done, that has made a difference.

[00:01:36] **Andrew Chrostowski:** Sure.

Well, I'll start from the saying that I began life as a physicist. So my original, work at Oregon State was in physics and engineering.

I spent a I spent almost 10 years in the Air Force doing command, control, communications, intelligence work. And so I always thought of things as complex systems and how to derive the solutions for that. So when I was at Space Division, I picked up a master's degree at USC, [00:02:00] University of Southern California, in systems management.

And always been, I think, of all business systems as complex activities. I've been able to apply that, frankly, in quality. operations, innovation, and ultimately in the digital transformation world. So it's been something that really has marked that. I just retired as the chairman and CEO of RealWear, one of the leading, wearable computer companies.

It's designed to address and connect frontline workers, around the world with, information that they need to work more productively and safely. I'm also a certified director for, National Association of Corporate Directors, where I serve on, several advisory boards. And, I am a, Digital Directors Founding Executive Member and Certified Qualified Technology Expert.

[00:02:45] **G Mark Hardy:** Now that's, yeah, that's, awesome. And I'm looking at, you know, we'll talk a little bit more. I wanna talk about RealWear. I also want to talk about the concept of a certified director. But basically, for a lot of people, I think in the cybersecurity realm, they look at.

You know, I have a technical career [00:03:00] and they've all focused on the technology. Often they come up through the ranks, if you will. And then all of a sudden, when you get to the C level, things change a little bit where you have to communicate differently, but now at the board level, it's an entirely new language yet again, isn't it?

[00:03:14] **Andrew Chrostowski:** It absolutely is. And in fact, it's one of the things that we talk about a lot at the Digital Directors Network, trying to help CISOs and other technology professionals in the digital space, be able to communicate in the language that matters. to board members. So if you think about board members general mindset, they're there to oversee the business, right?

They're not there to manage it. They're there to oversee it. They're looking at how to complies with regulations, how it complies with their strategy, the quality of management there that's being done. And of course, they're answerable to the shareholders and other stakeholders of the business. So today we focus as directors not only just on, on value creation writ large for the shareholders, but the larger concept of how do we work.

within [00:04:00] communities, with our employees, the actual industries that we operate. So it's a stakeholder perspective. So when you start talking to a board, you need to think about how they think about risk and value levers and speak that language so that they're paying attention and not getting tied up in some of the details that management would be very critical to

[00:04:21] **G Mark Hardy:** understand. And that's an excellent point that you brought up, is that as communications is being part of our requirements, we've got to have different messages. Obviously, a message to the staff for whom we were accountable and the people who report to us, we need to be able to communicate what it is that needs to be done and understand what they're doing.

To our peers, when we're looking at trying to help other people understand what do they need to do, like don't click on that, or something more complex, such as change the behaviors of your teams. That's another level of behavior. And then dealing with the executive team, who are responsible for, if you will, executing the strategy of the business.

It's more of operational, but at the board level, it's strategic. [00:05:00] And the language of strategy, at least from perspective of cyber security, would be risk. Is that a reasonable statement to state?

[00:05:06] **Andrew Chrostowski:** I think it's very reasonable. Again their object is meant to manage all the risks in the business.

So the digital risks, the cybersecurity risks. And by the way, whenever I'm talking about that, and especially with respect to digital technologies, it's the risk and the opportunity, right? Because you're actually managing three different types of risks there. You're managing the opportunity risk of not engaging with digital transformation creates so much value. You've got the cybersecurity risk of frankly, the bad actors that are out there trying to do something to your organization and take down your value system, whatever it might be, whether it's your personal identified information, the crown jewels of your IP, whatever it might be.

And then the third piece of that is really just the failure risk of these complex, interconnected, interdependent systems, these digital networks that can. frankly be taken down because of cascading errors within it. So those [00:06:00] are the three levels of risk that always are our concern of the board. And frankly, when you're a technology professional talking, you tend to focus only on the first narrow one, which is this idea of bad actors, but it's really much broader than that.

[00:06:12] **G Mark Hardy:** And that's very good insight because I think the danger we make, as you said, you tend to get trapped in one way of thinking. And then from that perspective, that's not what the language they want to hear. I remember the late Alan Paller, who is a founder of SANS had, was sitting at a pretty high level meeting where the number of senior executives and they had I think it was a CISO or the equivalent of a CISO give a briefing.

And as, after that person left the room, the most senior person kind of leaned over to the person. And Alan heard him and says, like, why is that person still on our staff? As if to say, I didn't understand a word that individual said, and why are we paying them? So, we want to ensure that it is understood.

That it is our obligation to learn to speak the other language, so to speak. And that's the reason for these podcasts, and for having you as a guest here, is to help our audience become better at their jobs, to be able to [00:07:00] communicate effectively. Now, As we look at some of the imperatives, obviously communication is one of them, but what about the concept of value creation?

Why is that a key business concept? And how does that work its way down into the CISO suite?

[00:07:14] **Andrew Chrostowski:** Well, first of all, I think it's critically important for every employee, whatever their role from the frontline worker all the way to the CEO and the management and then ultimately the board is what are the value levers of the particular business you're talking about?

Because those are the ways in which you sustain yourself. If you don't have a real firm grasp on the value creation mechanism for your business, you're simply not going to be a superior operation for any kind of sustainable period of time. So I think that comes down to, you know, what kind of business are you running?

Again, think of the boundary conditions from a physics point of view. It's like, what makes this system operate and what can be perturbed by it? So, you know,

when you think about the CISO's role today, think about all the values that, [00:08:00] that matter in these levers.

So, information for your customers, every ERP system, all of your customer resource. Management processes, right? You think about the IP that you store on your system. So many pieces of that value that are inside and have to be protected by your digital systems. It's probably the biggest area, but it's not the only area because you have to think about, you know, how as a CEO or as a board member, look, What other things interact?

Can we take orders? Can we ship? Recently there was a very large fruit company that was that was hit with a cyber attack. And, you know, they went back old school. Their contingency was, We gotta ship the fruit. We gotta ship the bananas before they, they rot. And so what did they do? They had a process in place to handwrite all of these things while they were down.

They shipped all their stuff to stores and they sorted it out later. Right, so understanding that for them, fruit sitting in a warehouse rotting is a huge problem for them and they had a [00:09:00] contingency built up to be able to keep that process moving despite a digital disruption.

[00:09:04] **G Mark Hardy:** And so the concept of value creation is important because this is how you justify a line of business or a new initiative.

If I say, hey, I want to compete for resources against some other proposal from some other executive, if I can demonstrate in creating more value for the organization than the competition, I more likely to be funded. Now, the challenge for CISOs and cybersecurity in general is often security is viewed, rightly or wrongly, is friction, and friction doesn't create value.

So how do we turn that around a little bit when we're communicating with senior executives to help them understand that cybersecurity really does create value? And it's more than just the preconceived notion of, oh, it's friction, it's slowing us down, it's adding costs, it's reducing our efficiency.

[00:09:49] **Andrew Chrostowski:** I love this question, G Mark, and I think that the idea of removing friction and creating value is absolutely fundamental to all well run businesses.

And so, [00:10:00] one of the analogies, I'll go back to my early days in the automotive industry in one of my first civilian roles working with Ford and GM and Chrysler and others. And there there was this thought process that, hey,

when we bring in real significant documentation for regimented how we build cars, how we do these assemblies, there was a perception and pushback that all of this was administrative, it's too much detail, it was too much discipline.

And they would kind of look and say, well look at Toyota they have all this mixed model flow and they're very, you know, adaptive manufacturing. And the reality was. It was actually the discipline of Toyota with respect to quality, documentation, procedure that was so well oiled into their system. It allowed them to have the operational flexibility to be flexible.

And so, you know, one of the key lessons is completely alignable with cyber strategy is you've got to make sure everyone understands that. All of this cyber hygiene, [00:11:00] activity, process, all of that aligns around to give you the flexibility to operate. It actually removes that friction and creates value.

And frankly, you know, it's, it may be that little bit of sand in the gears when you're running day to day, but when that car stops altogether and you're not able to do anything because your systems are down, that's when this idea of flexibility will come to the forefront and say, wow, I'm glad we had that in the background. So it does create value and it does give you back access to your value creation system.

[00:11:30] **G Mark Hardy:** And that's very good insight. And you touched on a couple of concepts that I think we'd like to go into when you were mentioning Toyota. One of them was the concept of culture, and the other is operational excellence.

I don't know whether we want to talk about it individually or separately, but but your choice. Also, important imperatives in our roles.

[00:11:47] **Andrew Chrostowski:** Yeah. No, no question about it. I think there, A high performing organization is intrinsically linked to a high, a culture of high performance. I really, I've never seen the inverse of that be true, right, for any [00:12:00] sustained period of time.

And so, you know, culture really begins with every employee being engaged and understanding the vision. There's a great book I just read that leadership is overrated. And you know, that the concept there within the Navy SEALs is one of their first exercises is to kill the leader. So if you're in a small team.

They'll end up in the exercise saying, okay, no your leader's now been killed. You have to complete the mission. And now you have this discipline within this

small, you know, unit cohesion that they all know what the mission is. They know what their capabilities are and they go off and execute anyway, right?

That you're able to adapt to those kinds of situations. It's rare in industry that we actually encourage people to have that same mentality of understanding what the objectives are, how to align around them. And, you know, move forward with high engagement, understanding the mission and feeling positive about it.

And ultimately that's what drives. You know, the feedback loop of a successful culture is when people understand what they're working for, that they're making a difference, and then they're able to [00:13:00] then make decisions that allow them to to execute towards that goal.

[00:13:05] **G Mark Hardy:** Yeah, and I think a lot of that culture and the decision making comes down to trust.

And as we develop a more mature relationship with our people, basically when you first start out and you got some, a new hire. Bobby the Intern, as we nickname him you trust that he's going to be an honest person, but he's gonna make a lot of mistakes because he doesn't know what he's doing and he has no experience.

And so we set controls, we set limits, a very tight reporting structure. And that works well until this person begins to understand and is demonstrated capabilities to execute, at which point it's more natural to sort of back out and go from a directing. to a delegating and finally just, you know, you got it.

Andrew, here's the job. Call me if you need help. Otherwise it's kind of, you know, what I like to think is the best boss you have is someone who just says, here's what needs to be done, a good or done and report to me if you need any requirements. Otherwise I'll assume it gets taken care of. And so as CISOs, we build that level of trust every [00:14:00] day by our ability to Ensure that the organization's critical resources are up and running, if you will, the value creation element of it through a culture element as well, by being able to communicate effectively the imperative of the importance of cybersecurity and why that little bit of effort on everybody's things to say, this is why we're doing MFA.

This is why we're doing that really adds a lot of value. And then that can push us toward the next term, which I had mentioned, which is operational excellence.

[00:14:26] **Andrew Chrostowski:** A quick story G Mark that kind of connects those two pieces on the culture and the operational excellence. It comes from my days in the aerospace management and was actually still wearing a blue suit at the time and I was looking at a company that had about 85 percent of the world's market share in a very critical military component and I was asked to go Investigate this company, make sure they were, you know, stable and doing well and that they need to take some technology transfer risk away because of this company and very well run company.

And they had pioneers and an SPC application at the floor level on. I remember talking to a young 19 year old wave solder machine [00:15:00] operator. And you know, the man kind of walked by and said, Hey, this is, you know, they're doing SPC here, blah, blah, blah, blah. Next stop. And I kind of stayed back and I asked this guy, I said, well, Okay.

What do you think of all this SPC stuff you're doing, right? And he looked at me and just with his passionate voice said, I love it. I absolutely love it. I was like, whoa Okay, that's the first time I've heard, you know, someone here saying they love something like this. I said, why do you love it? He says because before I used to be working away at my wave sounder machine And suddenly, engineers would show up, push me out of the way, say I was making bad parts, make adjustments on the machine, right?

Turn it back over and walk away. I always felt terrible about that. Now think if you were someone working in cyber security in the information technology department, if you've had that experience of something going wrong. And they said, but now with SPC... I watch my own data. I look and see when there's a trend happening and I call them to come fix my machine before I make a bad part.

The onus, the energy has gone from being the victim of a system [00:16:00] to being the owner of a system that helps collaboratively to make something happen. Think about trying to make an organization where there's lack of fear. Those IT professionals working deep in the bowels and late at night and all those things have that same sense of empowerment.

About monitoring a system and raising an issue and having no fear of having that, you know, be their problem, but instead having people come to assist before there's a disruption or before there's a critical event. I think it's, you know, the testament of how management creates that lack of fear and trust, as you mentioned, G Mark, that is a great step for culture in an organization that leads to operational excellence, which we can talk a little bit more about.

[00:16:37] **G Mark Hardy:** Right. I think W Edwards Deming would be very pleased with that type of an arrangement there, you know, with the total quality management. So as we talk about operational excellence, but also not just doing the job at hand, but how do we continue to improve?

We get into growth strategies as well. And when we look at growth strategies, we often say, well, that's. That's the job of the CEO. That's the job of the marketing department. They're [00:17:00] out or the new products department, but really how does growth strategy align with cybersecurity? And what is it that we could do to both deliver operational excellence as well as contribute to a growth strategy?

Yeah,

[00:17:10] **Andrew Chrostowski:** Great question, G Mark. And when I think about those two elements together. The first thing on growth is that there are several aspects of that, right? There is, again, think of a system, you know, think of a system you're trying to now create, you know, long term sustainable growth in this.

You have the question of whether or not you have, you know, the right product market fit for your service or your product, right? Do you, are you building the right thing? Cause otherwise, you know, pushing that becomes very difficult. And do you then have the systems to scale with your success?

There's a lot of stories of startups. that have, you know, failed because of their own successes, right? They're not able to handle the back end of all the demand. And so, I think in this, in the same guideline, when you start focusing on operational excellence, which is again, low variability, right?

What is a characteristic of a high operational excellence [00:18:00] business? It's processes with low variability, well documentation, adaptable, high communication, high trust environments. Those adjectives applied to an information system lead to this same idea. And again, if your growth strategy that is strategic relative to product sales or services, depends on certain digital functions being available, if you're not able to scale easily to that you're gonna, you're gonna inhibit growth.

And I think that's one of the big reasons we saw the push to cloud, frankly, over the last decade, was scalability became so much easier in a cloud environment, it did with on premise.

[00:18:37] **G Mark Hardy:** That's a good point. And so cloud and the move to that actually did enable a lot of business growth strategies, even to provide the capability for search.

Okay. Black Friday, we're going to sell a whole bunch of stuff, but we don't have to spin up all these extra servers for one day out of the year. Let the cloud worry about it. It's expand contracts. It works really well, which is sort of leads us into the next thought I had, which [00:19:00] is the concept of innovation.

And sometimes we see in the cybersecurity world, a lot of changes, things change very rapidly. And as a result, we may be more sensitive to innovation than business leaders that are in areas that things don't change that much. You know, a chemistry textbook hasn't changed much in 150 years or a mathematics textbook.

But, you know, any computer book that's more than a couple years old is probably obsolete by now. So how do we apply innovation as cybersecurity professionals to help the overall organization?

[00:19:34] **Andrew Chrostowski:** That's a great question. And when you think about innovation, that perspective there's actually, I think from the board level conversations, right, we think of innovation as a positive thing.

It's something we're trying to create. In order to have this environment to get an advantage over competition, to create a moat or an edge around our, you know, our business and the services that we're providing. Innovation can kind of have the opposite feeling in the [00:20:00] technology areas where you're thinking that, well, this is, you know, new risks are being introduced.

So, you know, AI driven systems here. Hey, it helps us with the way we could defend our systems, but absolutely enables. You know, greater attacking. And you think about now within this world of kind of democratized ChatGPT kinds of services, right? How much easier is it today to imitate a voice or a video to do phishing on or spear phishing with executives and things.

So I think technology folks react innovating. And therefore, the onus is on us to kind of counter that and business at the lower, at the board level saying, Hey, we've got to innovate because if we don't, somebody else will. Right? And so you begin to feel that stress. So I think you have to bring the idea of the positive.

It goes back to those three things I talked about before, you know, opportunity risk cybersecurity risk and then complex systems risk, right? And in the world, if you think of it as a Venn diagram, our IT professionals [00:21:00] are really in that complex cybersecurity risk area where they're worried about bad actors and the complexity of their own digital systems.

But they worry a little bit less about the opportunity cost. And so if they can shift that discussion when they're bringing ideas forward to the board around the value levers that bring into that opportunity costs, you don't do this, you will miss this opportunity. Or if you don't implement these kinds of controls, right, you risk having a major disruption in your in your operations.

Then you're

speaking their language.

[00:21:31] **G Mark Hardy:** And so that's excellent advice. And really what. What we want to be able to do is learn and then execute faster than the competition, because a lot of it out there is a matter of, yes, we could be innovative, but if everybody is exactly the same innovation rate, all we've done is keep up.

We can go ahead and go for operational excellence, but if everybody in our industry is excellent, well, then you're just keeping up. But if you can do. A differentiation, if you could then be able to demonstrate that as [00:22:00] security professionals and business leaders, and that's another important Venn diagram that I think as a CISO, we have to recognize and then add to that maybe a communicator because you could be really good at one and or both, but not be good at communication, but to be effective at our jobs, we need to do all of those.

And so then I think the intersection, but also we've got to be the union of all that stuff. Helps, I think, in terms of helping understand, are we charted on the right course? And, you know, as we look to do things and the like, you had an article that you published recently that I really love the title.

I want to mention it. It's called the Intention Deficit Disorder, or IDD. And you'd mentioned with no offense made to anybody who may be suffering from an ADHD or some other you know, medical condition. But tell me a little about your thoughts about what. What was your idea behind intention deficit disorder?

And oh, by the way, maybe I resemble that remark because a lot of us might think sometimes we do. Yeah.

[00:22:52] **Andrew Chrostowski:** No, it's look, I, every year since my early twenties, I've sat down in the last. You know, two weeks of the year. And I think back about my [00:23:00] year's goals. Did I achieve? What did I achieve? How did I achieve?

What can I learn from over my major failures? What do I want to accomplish next year? Right? And so in this period of time, when you're everyone's focusing on what are my goals for the next year? What do I want to improve? What I want to work on? What I found is that in my reflection, looking at how, you know, number of articles where people failed in executing this, right?

The time to go get your gym membership started is in February, not in January, right? Because the gym would be crowded for the first three weeks of January, but wait until February. And now people are back to their own habits. And I realized it was really intention. This idea that we have a... Major intention, we focus on what it is that we're concerned about.

Right? And if we have, you know, sufficient intention and attention on what we're doing, then we will make progress. And too often, I think in our society in this fast paced social media kind of world, right? We're constantly being distracted by other things. We miss out on having [00:24:00] that firm intention to go get something done.

And if we maintain that, lower our focus, fewer things, get those things done, then I think that we have a much greater chance of succeeding. And so, it was my way of trying to capture an insight I had from my own reflections on... Making sure that as I entered 2023, in this particular case, that, you know, my intentions were you know, very clear on what I wanted to accomplish and sharing with everyone else to challenge them to really ask themselves, is it a goal or is it true intention to get something

to happen?

[00:24:35] **G Mark Hardy:** And that's very good insight on that. I know that. For a lot of us, we start out and they said, you know, the road to hell is paved with good intentions here, but also it's not just a matter of day to day execution. I mean, like most people, I've got my daily list here and I'm scratching things off as they get done but we're talking a little bit more.

Medium to long term. As you mentioned, kind of doing an annual review. What went well in the past year? What could I be doing next year? Excellent [00:25:00] idea. Even better, if you could create a mastermind group where you have other people with whom you can be accountable. And whether it's just something as simple as, okay, if we are going to join the gym, or we're going to go out and run, or we're going to go, whatever it is you happen to go learn something, is that having some sort of a peer or social, you know, pressure might be the wrong word, but ultimately that's what it becomes, down to is to say, hey, I'm going to keep doing it.

And so you move from intention to action by being able to eventually internalize that. So I, I was on travel several weeks ago. I was over in Madrid and one of the things I want to do is brush up on my Spanish. Not to spend any time on me here, but I found that little Duolingo program was kind of nice and because my Spanish that I took was in ninth grade, so it's been a long time.

Hola, que tal? And me llamo Paco, but I don't think it is. But what I found though, is that it kind of encouraged you, Hey, every day you got a streak going Hey, you can just do one more. Hey, there's a few hours left. You could finish in the top [00:26:00] so many and you promote to the next level and things such as that.

And so this is just an app that has combined sort of my intention to say, Hey, I want to gain better fluency. add an important language, Spanish, with my day to day activities, and so now it's a sort of a thing where it's now internalized, and... What we can do professionally is not only incorporate that in our career planning, but also in our counseling and our mentoring with the people that report to us.

Because one of the problems that I see happen for managers is, and it's a leadership issue too, is that we're been around long enough. We got some of the gray hairs here that say, yeah, we figured this stuff out. But a lot of the people that are. Coming up in the next generation, haven't had a chance to go through that yet.

And maybe nobody's ever sat down with them and said, Hey, here's how to do some longer term planning. Here's how to go ahead and create an accountability loop. And so there are ways that we can be better leaders for our [00:27:00] people by sharing not just the technical expertise or the to do list of make sure this gets done by the end of the day, the end of the week, but also help with the transformation for people to be able to better understand how to make their lives more effective and more meaningful.

[00:27:14] **Andrew Chrostowski:** I think you hit on two really important things that I would unpack on that. One is this idea of accountability partnership, and one is on the gamification of systems. And both of these have you know, relative importance to technical and cyber professionals. So just a quick story from my Air Force days.

I did a lot of triathlons, and so I trained, I ran in the morning, I swam at lunch, I would bike 20 25 miles after work, and I had a training partner. And there were a lot of days when you get to that end of the day, you get back to your apartment, you say, Oh man, I do not feel like, you know, getting on that bike for 20 miles, but you knew that your friend was waiting out there to meet with you and go, and so you get on the road and 10 miles into your ride, you'd lean over and say, you know, I really didn't want to go today, but I didn't want to let you down.

And he looks at you and said, well, I didn't want to go today either, but I didn't want to let you down. Right? So there's this idea of [00:28:00] mutual accountability partnerships that really, at a professional level, boss to employee to employee, whatever have value. Right. That's that culture piece of performance.

But the gamification thing is really important. We've all seen in all of the apps and social media apps doing this as well, is trying to make sure people. You know, feel that accountability. And so you can do that with cyber security tools. You can do with cyber security training, you can do with education.

So there's all these little lessons about how human beings interact with each other. We care about those interactions. And so those are lessons that can be applied in a larger context. So I love those ideas of accountability and gamification relative to making a system change in a culture change.

[00:28:39] **G Mark Hardy:** Good insight. Thank you very much on that one. So Yeah. As I say, I like that article. There's a couple of quotes that I had read that you had written that I'd like to share. And the first one was this, the time for a digital strategy is past. What is needed today is a comprehensive strategy for a world of digital opportunities and existential [00:29:00] cyber risks.

Now, why are we going to throw out the, are we throwing out the baby with the bath water by saying the time for digital strategy has passed? Let's unpack this a little bit and let's get inside your thoughts.

[00:29:10] **Andrew Chrostowski:** Yeah, you know, I feel it's a little bit like the comment that Obama made during one of the presidential debates, where he says the 1980s is calling and they want their their strategy back from in terms of security risks.

And I think what I mean by that is that there was a time. In the early days of Amazon, in the early times of, sort of, those of us who remember you know, what a dial up tone sounded like, right, when you're connecting at 300 baud that was a time where strategy meant something relative to this big thing that's happening, the internet, going to a browser, the World Wide Web, but my point is, The asteroid sort of hit already and, you know, just some dinosaurs don't know it yet.

So every business, in my view, is already involved in a digital link in their value stream. You're hard pressed to pick out any business that doesn't have a digital dependency on their value chain. You know, unless you want to talk about your [00:30:00] neighbor's lemonade stand, you know, next door or something with the cash business that nobody cares.

You know, so, so digital strategy of thinking about, hey, how are we going to go digital? That's gone. I think that time is you're looking in the rear view mirror while you're, while your competition is way ahead. Today's world is all about this interconnected, interdependent, complex systems.

Right. That are working together and that creates huge opportunities for how you can transform the way you deliver value to your customers in whatever way you deliver values. But it also means all of that complexity, all of those new tools and access points. Create huge cybersecurity risks for you, which can be huge penalties if it's a G D P R kind of penalty that you weren't aware of, or it creates you know, under-reporting that we now know that the SEC is gonna be leaning heavy into that come 2024.

And so I, I think really it's not just strategy is no longer. A reasonable conversation to have about general you know, computer strategy. And now it [00:31:00] really is about what are we going to do specifically about these huge transformations that are happening? I think today's boardrooms are talking about AI a couple of months ago, they were talking about blockchain, right before that they were, so there's always these things that come in that need to be incorporated into a comprehensive strategy that also creates.

You know, significant risks that need to be

managed.

[00:31:22] **G Mark Hardy:** Which also suggests that comprehensive strategy is dynamic. It's not something you do once every 12 or 18 months, because that might be the life cycle of what we're looking at. You know, it's, they mention, you know, and a lot of shows, G Mark's Law, and then you go and say, okay, fine if we go back in time, and we take a look at 18 months ago, who was talking about ChatGPT? And 18 months from now, Windows 10 is going to be officially obsolete. So what we're doing now is we're shifting to a ongoing continuous strategy, so to speak, allowing us to incorporate new ideas, new concepts, adapt to the environment as new forces come [00:32:00] in and then address those risks as well.

And to do so, we've got to. Stay on our toes and you can't just rely on if you will yesterday's training and yesterday's capability So the other quote that you had which was sharpen your axe. It sounds almost like Stephen Covey's seventh tenant Sharpen the saw but tell me a little bit about your story behind sharpen the axe

[00:32:19] **Andrew Chrostowski:** Sure, sharpen the axe comes from my experience in oregon with my dad who was a forester and We would go out every year and collect several cords of firewood in the forest So we'd have you know stack with three or four cords of firewood that have to be split And of course my job as a, 14 year old was to, you know, go do that work while dad watched football.

And I'd be working away and of course you want to go on a date, you want to go to the movies, whatever it is that you're trying to do. So you'd be working as hard as you can and you'd be hitting. And the longer you're working with that axe, the harder and harder it would be to split that wood. And at a point where you're really struggling, the sliding door would open, and my dad would glance out and say, Stop, go sharpen the axe.

And you didn't want to stop, because you wanted to get done. [00:33:00] But you do it, you stop, you sharpen the axe up, you go back to the pile, and suddenly the wood's flying apart again, and you're working away, but you get head down into it, and pretty soon, it's getting harder and harder to split the wood, and the window would open up again, and it's like...

Go sharpen your axe. And so you've stopped. So the point is that really when we get into a task, it's so easy to get myopic about what we're doing, that we lose context of What makes it easy to do this? In this case, you know,

sharpening the axe makes that wood split apart much with less force. But there are a lot of applications in life, you know, where we just keep digging in and instead of asking ourselves, Hey, how do I make this easier?

And think about this from a technology perspective. How many, you know, tools have IT professionals created for us now that are equivalent of a sharp axe? So I think that's the thing that we kind of, you know, build into in terms of You know, doing things better and continuously focused on that, but not getting tied up with the fact that When the level of effort gets [00:34:00] harder, not to back off and think about a different way to do it.

[00:34:03] **G Mark Hardy:** And I think to emphasize that point, it's in addition to not just the processes that we have, which we want to keep sharp and obviously one analogy could be keep your software up to date, but also our own skill sets. And so investing in our own professional education, whether it's formal, whether we go off and get a university degree.

Whether we go and get a commercial certification or do what we're trying to do here, which is to provide a body of knowledge through a podcast or a YouTube videos that people could go to and say, wow, I learned something useful. It's all a matter of staying engaged in that. I know that my partner here at CISO Tradecraft, he says he goes through, I don't know, something like 14 or 15 podcasts a week.

And like, how do you find the time? He says, well, Plays them at 2x, and after a while, you listen to things at 2x. If the speaker is good diction and they don't have a lot of fillers, it works, and for his morning walk, he can knock out, well, in a 30 minute walk, he can knock out an hour's worth of podcasts, and all of a sudden, it adds up, [00:35:00] and what we find then, is there's a cumulative benefit toward sharpening that axe, although it might be dulling, so to speak, against the last Bit of wood that you've chopped.

The reality is that the habit of doing so becomes a sustainability element. Much like that accountability where we go ahead and we're gonna go do the run, or we're going to go work out or do the ride even if we didn't feel like it. Because once that's internalized, I think it's really made a big difference.

And so that's where we wanna get to. Where it's nice if I have an accountability partner, but if I don't. I'm still going to do it anyway. And because you look at the way that some people happen, I mean, how do you get an accountability partner for Elon Musk? Like who's going to keep up with the guy?

And so as a result, some people have to be self driven, not to say we could all be like Elon but we could learn a little bit from his behavior.

[00:35:47] **Andrew Chrostowski:** I would just say one more thing on that topic is in what Mark Twain said more than a century ago is even more true today. He said, never let school get in the way of your education.

And today, there is so much more to learn. As you [00:36:00] said, textbooks today in many subjects are obsolete before you get to them. So really, college today is more about learning how to learn. And learning how to think in a reasonable way than is about a specific mastering a topic because by the time you graduate that topic, you know, the world experts in that topic aren't teaching it, they're doing it somewhere.

And so, I think that idea of, you know, continuous education, leaning into Coursera, leaning into online tools. Podcasts, other kinds of things where, you know, lifelong reading that's I'm a big fan of the Read to Lead podcast that, that focuses on, you know, leadership is about experiencing the failures and successes of others and not having to do it all yourself.

So. Great

point there.

[00:36:40] **G Mark Hardy:** That's excellent. Now we're coming down to about the last 10 minutes of the show. And there's two things I wanted to cover. I'm going to jump to the one I think is the more important of the two. And if we have time, we'll come back to the first and let's talk about the Digital Directors Network.

The Digital Directors Network. Well, you've been involved in that and well, just tell me a little bit more about it because I was kind of fascinated by it. The more I read about it, the [00:37:00] more I'm saying I want to pay. I want a piece of this.

[00:37:01] **Andrew Chrostowski:** Yeah. So, so the Digital Directors Network started in about 2017.

I got involved in it very early on as an idea at the National Association of Corporate Directors in 2018, where I met Bob Zukas, the CEO and founder, and I became a founding executive member of this organization whose focus is CISO. Trying to bring, you know, digital savvy and cyber security experience

into the boardroom because we feel that is a unique and different kind of risk management than just all the other risks that people manage all the time.

And so, you know, there's this idea within boards and believe it or not, 25 years ago before Sarbanes Oxley, it wasn't, there wasn't a need for a qualified financial expert to be on a board's audit committee. So think about this, right? You're, Hey, we can manage, we know how to look at a financial state. And then of course, then the financial crisis hit and suddenly government says, no, you need to have a qualified financial executive on your board and in your audit committee in order to understand the complexities of all these things are [00:38:00] happening with the financial malfeasance that went with Enron and WorldCom and all of that kind of stuff.

Flash forward to today, you've got board members out there who will say we manage all kinds of risks. We don't need to have, you know, a qualified technology expert in our board. You know, we just need to be able to ask better questions. And in a summary, digital directives is about, well, it's not just about asking better questions.

It's about actually understanding the answers and being able to go down to the next level. So we deal with the problem from both sides, helping CISOs and other cyber executive professionals. Speak the language of boards and be ready for board governance opportunities that we think will be happening, much like you saw the initiative for women getting into the boardroom and other diversity of thought and equity happening in the boardroom.

And the other side is board education, helping them understand the dynamics of these risks, the opportunities, and The the nature of what they need to oversee.

[00:38:56] **G Mark Hardy:** Now, do you think that the SEC missed something when [00:39:00] their recent guidance, which came out effective in September with regard to cyber security and boards, where they struck that provision that boards had to document what their cyber security expertise was among their membership?

Or do you think it's just something that they didn't want to throw too much too soon and that's going to come later, or do you think that the writing is on the wall and that a prudent board will have some cybersecurity expertise, whether or not they're told to do so? What's your read on that?

[00:39:26] **Andrew Chrostowski:** Yeah, in the end, there's, I think that the die has been cast and we just haven't gotten there.

I don't think the SEC went far enough without specifying and have that kind of, of technical governance on your boards. But I think it's going to get there in the future. I think there's a lot of resistance from other organizations and existing boards who didn't want to be you know, pressure in this area. But this, the nature of the challenge that we talked about, right, the cyber security risk, complex system risk, opportunity risk are going to force ultimately that to happen.

And we'll look back, and I don't know if it'll be five years or 10 years. And people [00:40:00] have that same perception that, you know, if today you said you don't need a financial expert on your board well, they'd say, well, of course it's required by legislation today, but of course, if that's a bad idea, of course you do.

I think five, 10 years from now, the same feeling will be, of course, in a world that is so digitally connected and interconnected, you need to have this kind of expertise at a deeper level on your board of directors. I think that is inevitable.

[00:40:23] **G Mark Hardy:** Good insights. Now, one of the things that I know the Digital Directors Network have is some courseware, and one of them is a Boardroom Certified Qualified Technology Expert, or a QTE.

Could you tell me a little bit about the concept of what is a QTE? Is that a board person getting smart about cyber? Is it a cyber person getting smart about board? And then how would somebody investigate that a little bit further?

[00:40:44] **Andrew Chrostowski:** Well, first of all, I encourage everyone to go to the Digital Directors Network and find out more about it.

There are classes for the... Certified Quality Technology Expert 501 virtually every month. And so they can go there, sign up it's delivered both in online modes and it is also delivered [00:41:00] in person. So depending on your schedule, you can do that. We also have an annual conference. And the next one is Domino 24 happening May 15th and 16th in Chicago, where at the University of Chicago, you know, the best voices on cybersecurity and governance come together.

And we really have conversations about what is, what's happening in this space between regulation, between best practices, between emerging threats and opportunities. So, I'd encourage your listeners to take a look at what's going on at Digital Directors. And that QTE class is mostly focused on cyber professionals, CISOs, and CEOs who want to be in the boardroom.

But we've had a lot of board members who have come in and said, I want to understand what my part of it is. So we've worked, you know, both sides of that equation.

[00:41:42] **G Mark Hardy:** Interesting. And it does sound worthwhile. So that's kind of on my list that you talk about the intentions and things like that. I put that kind of on my list of things to look into.

for next year. So we're getting close to the show. So let's do a little bit of wrap up. So we talked a little bit about imperatives, the idea of value creation, being able to help [00:42:00] the organization generate more than you've put into it, if you will, creating value, the importance of. And why that matters and our ability, not only with our relationships with the people to whom we report and work with, but also the teams that report to us.

Operational excellence, the ability to deliver above and beyond the standard of mediocrity so that every time something is done from security or within the organization, it's done correctly. And it's done so well that people like. We looked at growth strategies, the ability to be able to support the organization as they go ahead and get into new lines of business or expanding what they're doing and security being an enabler for that rather than, if you will, sand in the gears.

And then innovation, why we're constantly dealing with innovation. in cybersecurity because of the rapid nature of change and also therefore why innovation would be important in dealing with other elements of the organization from a cybersecurity perspective. We mentioned your intention [00:43:00] deficit disorder article, which I loved again, the title of that.

And again, I'll repeat your quote. The time for a digital strategy is past. What is needed today is a comprehensive strategy for a world of digital opportunities and existential cyber risks. And and we finished up with the idea of sharpening your ax and then the opportunities that are presented to cybersecurity professionals through an organization called the Digital Directors Network.

It's the website, digitaldirectors. network using that. And then you can find information there, including, as we said. That QTE course, is there anything else that I didn't think of before we wrap up the show?

[00:43:36] **Andrew Chrostowski:** No, look, thanks very much for allowing me to talk on a topic I'm passionate about. The world is changing.

Obviously we are moving forward in a world where everyone needs to be connected. And it's one of the reasons why at RealWear we focused on the frontline connected worker, because there are over 2 billion people out there who are, you know, today working with their hands on the front lines, whether they're a surgeon or a mechanic.

That need access to [00:44:00] the same information systems that we've been talking about for this last 45 minutes of knowledge workers. And so I think that the world is going to be completely comprehensively connected here with these digital opportunities. And for your listeners, the folks who are securing that digital framework, it's so important for the value lovers that we're going to have available to us in the years to come.

[00:44:21] **G Mark Hardy:** Well, thank you very much. For our audience, you've been listening with Andrew Krostowski. And I'm your host, G Mark Hardy. We hope that you've enjoyed this program. If you like, please follow us on LinkedIn. If you're not doing so, we do more than just podcasts. We have what we hope is a high signal to low noise ratio, steady stream of information to help you with your career and look for us on.

YouTube, if you're not doing so already. And now I understand why I always want people to follow you because it helps us get rid of the ads we don't want to, and we get better control. So you help us out and you help yourself out. It doesn't cost you anything to do so. And don't forget to share with everybody else where you get your good ideas because hopefully it's here.

We're always willing to listen to you. Give us a note at [00:45:00] CISOTradecraft. com or connect to us on LinkedIn. Otherwise, hopefully you have a great and a safe week and until next time, stay safe out there.