#123 - Accepted Cyber Strategy (with Branden Newman)

[00:00:00]

[00:00:12] **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 today we're going to explore how you can build an accepted cyber strategy that executives will appreciate.

Well, let's start off in by defining the word strategy. The Collins Dictionary gives a couple definitions. A strategy is a general plan or set of plans intended to achieve something, especially over a long period. Okay. And strategy is the art of planning the best way to gain an advantage or achieve success, especially in war.

Well, okay. What can we learn from these two definitions? Basically, strategy equals planning to obtain better outcome, and therefore, if we're not planning, then that [00:01:00] means we really haven't built a strategy. It's like the old phrase that goes, if you fail to plan, you plan to fail. So what are the things that we plan about?

Michael D. Watkins wrote an article for the Harvard Business Review, and he demystifies strategy and talks about it saying think about it in these four questions. Who is our first question? Essentially, we need to know where customers are and so we can create value for them. And this question is generally answered by the marketing team through the creation of customer profiles.

So therefore, that's not really strategy. He goes on to say what is there second question, starting to sound like who's on first? Right? , we need to know that we're going to achieve something and so what is it that we're going to achieve To address this question, executives will create mission statements and goals for the organizations, and these items might be broken into objectives and key results and things such as that.

So the what question though isn't about strategy either because it focuses on creating [00:02:00] effectiveness and efficiencies in our programs and projects. Okay. Watkins says, why is our third question? And we do know why

employees are going to be motivated to do the work, and we can find out why for the organization by looking at vision statements for the company and tying incentives into things that motivate others.

Now note, it's usually a form of rewards or ideology or coercion or ego, but the main point here is that while why still isn't the strategy question to focus on, we're running out here. So that leads us with the fourth question from Watkins. The how question, how should resources be allocated to accomplish the mission?

And that is a strategic question that we need to answer. And we have to tackle that. So let's dive in. For most companies, the mission of the organization is to create long-term profitable growth. And if we want focus on long-term growth, we need to first understand how the company makes money. And to do that, let's take a look at the financial statements.

For example, you could look at year-end financials [00:03:00] in any publicly traded company. And within those statements you'll see information about where sales and revenue are derived from. You can look at P and L profits and losses by business segments, and you might find, for example, that the credit card division makes 80% of the profits of the entire bank and now you know to dedicate time with that business segment.

If you want cyber to be relevant to protecting corporate revenues, and as you look deeper, you should ask yourself, what are the critical business processes and IT systems that support the credit card division? Now, once you find out those critical systems and process. Then need to go ask the business owners what their strategic objectives are, what tactical issues make it difficult for them to work, and what is the current business environment that they face.

Once you understand the business perspective, you can design a future state of what their system should look like. Essentially, you know, your executives want something to be cheaper, faster, and better, but you kind of need a clear definition of what it means to be done. And that way you can avoid [00:04:00] building the wrong thing.

Once you've created desired future state document, you should perform a gap analysis to show the work that needs to be done from where you are now, to where it is you want to achieve. You create a list of activities to perform, and this list should show each activity and the resources required.

Resources could be people, technology, time, and money. The end result is you produce a list of perhaps 30 things that you can show the executive team essentially say, here is a realm of possibility for us in the next 12 months, and you can then point out that you've been allocated enough resources to implement the top 20 items on the list and based on various stakeholder interviews, we think that this is the list which is most important to the organization and you ask the senior executives team, do you concur with how we prioritize this current list? Or do we need to move certain items higher or lower? But remember, anything below that cut line, that's number 21 to 30 is not going to get done in the next 12 months given our current resource [00:05:00] constraints.

Are we okay with that? Because if not, we either. Add additional resources, or we have to accept the risk of things not getting done. And if you do things like that, you can create an effective dialogue that executives can participate in, to champion security. Okay. Now that we've talked a little bit about strategy, and I've had this poor gentleman just sitting here on hold for a few minutes, I'd like to welcome Branden Newman to the show.

Branden, welcome to CISO Tradecraft.

[00:05:27] **Branden Newman:** Thanks a lot. Happy to be here.

[00:05:28] **G Mark Hardy:** Glad to have it. Hey, can you tell us a little bit about yourself and how you became a CISO?

[00:05:33] **Branden Newman:** Sure. I'm the CISO of MGM Resorts International right now. I started out originally, I guess I've been a geek my entire life, so I knew I wanted to get into something technical. I joined the military at 17, the Air Force started doing, standard IT stuff, switching and routing, working on help desks, just kind of rotated through all of it.

After taking a short detour over to the Army to be a, a Black Hawk pilot for five years, I decided that [00:06:00] wasn't my long-term goal and I was a geek at heart. So I came back into, back into cyber, worked my way through essentially 15 years of Department of Defense ending up in cyber command. And at this point I got recruited over to a, pharmaceutical company, a Merck Group out in Germany to, to build out their security operations center.

little did I know, I, I didn't know how little I knew at that point, as I jumped off of just running, you know, a, a massive soc really focused on, nation state actors

and things like this, getting into the corporate world, which was a whole different environment. And that, kind of kicked off my career.

eventually, becoming a CISO, of Adidas and now of, MGM Resorts.

[00:06:42] **G Mark Hardy:** Now that sounds like some pretty huge brand name. And I, I look at that and you go, whoa. And then of course, first of all, you say, you know, you got any good deals over there when I get to Vegas for, for blackout and Defcon. But more to the point, I think, for some people who are thinking of aspiring to be a CISO, some of us kind of start out in the trenches, as you said, many of us [00:07:00] begin in the military, which I think is great, and, and I did that as well.

Although when I was there, they didn't have cyber in the military. I remember, that, that was always my frustration. It's like I was born too soon. In any case, when you were able to go ahead and move up to those bigger jobs, was that your idea? Did they recruit you? I, I mean, to me, well, think a lot of people, they get a little bit intimidated and go like, whoa, MGM resorts or something like that.

But what was your thought process?

[00:07:28] **Branden Newman:** I wouldn't say that I really set out to be a CISO. I was, like I said, I was a real technical geek, basically. I loved solving problems. I loved, you know, incident response, figuring things out. so it kind of fell in my lap. It's one of these, deals where, The, the expert that's doing the best job just gets promoted to the manager.

And then next thing you know, I'm a VP under the CISO figuring things out. And then I, I think about that time when I was in leadership one level below the CISO, I said, you know, I want to be the guy making the decisions one day. You know, you think maybe you disagree with a [00:08:00] few ways that things are going and you say, I think I could do that job, fairly well and give it a go.

[00:08:06] **G Mark Hardy:** and here you are. So congratulations. And, , of course, enjoying the ride.

[00:08:10] **Branden Newman:** that's right.

[00:08:11] **G Mark Hardy:** So a little bit earlier we talked about strategy and it's all about the how. And so how do we take the resources of a company,

whether it's a publicly traded company or even a government entity or military, or a nonprofit. and then accomplish the mission.

Can you tell us about your approach toward building an accepted cyber strategy?

[00:08:31] **Branden Newman:** Well, it starts with just learning the, the business. So every company that I've worked for, , including the military, so the, the military, pharma, retail, and now, hospitality, entertainment. each one of those has been completely unique. There are of course, some foundational items that are the same across all companies, but if you really want to get beyond just the very basics in cybersecurity and build a an effective strategy, the first step in my mind is learning the company inside and out.

So you can't just apply [00:09:00] a standard template. You need to know what makes the company tick and how the company makes money. How reputation affects the company. Just regulations. There's so many things to learn about the company itself, to decide how you're going to derive a strategy. And I don't think there's really a one size fits all when you're applying a, a cybersecurity strategy to a company.

[00:09:19] **G Mark Hardy:** And that's an excellent insight because I think a lot of folks that we start out in the technical world and we say, Hey, I'm going to be the best technical CISO out there. And that's almost an oxymoron because reality is you're, you're. Getting up into layer eight, you're there in the politics layer, and that's how things get done when you're interacting with people and you're trying to get your budgets approved when you're trying to pitch stuff like that, it becomes relationships, communication skills, and the communication is learning to speak the language of management and the leadership team.

[00:09:48] **Branden Newman:** That's exactly right. I would say that, my technical skills are used very rarely these days. And if I had to argue, a skill that's most important, communication skills and [00:10:00] being able to influence people makes a CISO effective. Of course he has to understand everything underneath that to some extent.

But at the end of the day, when you're running these very large teams, you're going to have to trust your team. And the technical experts are, hopefully better than you are at their individual, silos. but at the end of the day, communication is where it's really at.

[00:10:19] **G Mark Hardy:** I, I concur. Now in my, you know, intro that we did in the show here, we're talking. What things that you need to focus on, and one of the things we see a focus for understanding is financial statements. So let's take a CISO who's really good technically and knows a lot about cybersecurity and is now starting to work their way into understanding this management communication.

They've really never taken business classes. , what should they look for in a financial statement? How do you, what do you look at other than just a bunch of numbers.

[00:10:47] **Branden Newman:** Yeah that was exactly like me, right? So I came from technical side in the military and jumped into to the business, corporate side, and I really had no idea. So there was a lot of stumbling along the way. Of course now I've built a, a [00:11:00] routine as I started a new company to read their mission and vision, start there, read their corporate strategy, but really as you said in the intro, all roads lead to how the company's making money.

And that's really what's going to matter at the end of. So when you start checking out the financial statements, I've been very surprised actually in some of the companies I've worked for. You go in there and look, and what I'm looking for is, you know, what are the sources of revenue, right? Are they coming from, B2B?

Are they coming directly from consumer? Are they coming in certain, , Specific business units and not others. And it's really surprising outside looking in, you may guess certain things, but once you really start digging into those, you know, PNLs of various business lines, you'll understand, , exactly where they're making money.

And it'll let you speak to those executives in a, a very intelligent way that they understand, because you better believe they know those things inside and out. And if you want to gain trust with them, you also need to know them.

[00:11:54] **G Mark Hardy:** Now, have you ever seen anything in a financial statement that changed your focus as a CISO.

[00:11:59] **Branden Newman:** [00:12:00] Yes. I, I would say when you get a new position, you immediately, you know, your, the, the gears start turning in your mind and you think, oh, I'm going to go in there. And we definitely need to protect these things. I assume these are the crown jewels or those are the crown jewels, or this is the most important.

The things that have surprised me the most are just where the revenue streams are coming from and how I need to readjust to what my preconceived notions were coming in and what the reality on the ground is, because it's not always what the surface level appears to be.

[00:12:29] **G Mark Hardy:** That's a good point. So let's say we've looked at the financial statements as a CISO and we get a good understanding of how the business or organization makes money, and then which business segments create the most value for the company, which is really what we're talking about there. What, what's, what's keeping the lights on?

What are the next steps that you should follow?

[00:12:47] **Branden Newman:** Well, you're kind of, then pulling the string, if you will. So once you, once you get to know what, what business units you need to focus the most on, you get to know first the leadership. You start to understand their business processes and [00:13:00] how. I like to follow the money from the time I imagine, you know, a customer comes in, they're paying here, the money's traveling through all the systems, eventually, stopping here and sometimes gets into the bank , you know, so we follow this entire string to understand the processes and what the criticality of those are, and start building a program around that.

And, and taking that forward.

[00:13:23] **G Mark Hardy:** I'd seen that. Great advice. Now, any other additional tips you might define that help make that route go successfully?

[00:13:30] **Branden Newman:** Well there is some connective tissue in companies also, so you definitely cannot, , only follow the money. So this. We'll let you down. If you do this 100%, you need to fill in the gaps also, right? You need to protect your, your employees. That's a big piece. And you need to protect reputation because reputation kind of crosses all the business lines and that, that really has a big impact.

And I would say that. Obviously you can build the core of your strategy based on this whole follow the money type of principle, [00:14:00] but you need to make sure that you fill in the gaps on all of these kind of edge cases that will be protecting the employee base and in protecting the reputation of the company overall.

[00:14:09] **G Mark Hardy:** Yeah, and you've mentioned reputation a couple times, and I think that's very important because reputational risk is separate and distinct from financial risk, although ultimately that can pour itself into financial risk. If we think about companies that have had very bad publicity or something's gone horribly wrong, we realize that, it doesn't make you want to ban some, , you know, recently, , if you will, Silicon Valley Bank. Let's imagine that the run on the bank was mostly a reputational problem. The bank could have been fine, it could have been recapitalized, they could have done things, but once everybody started cashing out at the same time, it kind of all went, sideways and after that. So, I, I think your point is well taken on reputation.

[00:14:48] **Branden Newman:** Yeah, and reputation's kind of a double edged sword in my opinion I guess, cybersecurity practitioners spread a lot of fear in general and reputation's kind of our go-to because it's a gray, , kind of a gray area if you will. So we can [00:15:00] always say, Hey, reputation's going to take everything down.

But if you look through history, you know, everything from like target breach to to Sony, et cetera, you'll see that, reputation. While it can take certain companies down, other companies are fairly resilient to reputation hits. So this is where, again, where you need to really learn your company and understand how reputation plays into the overall strategy.

[00:15:24] **G Mark Hardy:** So at this point we've looked at the financials, we understand. What's critical, where the primary sources of revenue are coming in, what adds the most profitability to the bottom line? We've also considered reputation. What is it that could cause things to go sideways? Even though your numbers may look fine, if the reputation goes down, and of course, cybersecurity and having an incident is a really good way to have a, a reputational problem at this point.

Now that we've sucked all this information in our brains, we've done some thinking about it. What's a good way to go about getting executive buy-in into cybersecurity?

[00:15:58] **Branden Newman:** Well, this changes also [00:16:00] company to company, but generally speaking, you have to find a way to build trust with these executives. You show them that you. Understand the company, and we already covered that. You need to really know the mission, know the vision, know the financials. Once you start talking in their language and building trust, this is the best way to actually get your objectives done.

On the flip side, if you come in there just saying, I've reviewed this place and we need to put in MFA and, solve a million vulnerabilities and start locking down these employees, you'll get exactly the opposite reaction. So go in there with an open mind and try to build trust with these guys. And you're, explain that you're there to help and you're there to, hopefully even drive profit one day through a differentiation to your competition.

[00:16:45] **G Mark Hardy:** Yeah, and and that's a very good point because we can do things you couldn't do before. I mean, just think about something that we take for granted, being able to sell on the web. Well, if you didn't have. Secure communications with TLS and we didn't have good shopping carts and PCI [00:17:00] compliance and things such as that.

We'd have to have a storefront someplace or a mail-in catalog. And that's a very inefficient way of doing business, particularly if your competition's doing it. So in a way, Security enables new elements of business. And, and so that's an important thing to remind folks is that we could do stuff that we couldn't do before.

Now why do you think, for example, cyber gets ignored and, and what are things that might help you overcome business objections if you're just not getting the communication right. What are we doing wrong?

[00:17:28] **Branden Newman:** Yeah, I think in general cybersecurity practitioners are doing a couple things wrong. First off, we, we learn. Theory, if you will. So we learn all these frameworks. We go to school, learn how you're supposed to do things, and we come with this kind of perfect template and we apply it to a very imperfect business world, if you will.

Anybody that's been a CISO or worked in any corporate environment understands that there is. Virtually no perfection, in these operating companies. So I think that we, we try to kind of fit [00:18:00] the round peg in the square hole, if you will, without really understanding the overall setup. And to get that done, we usually spread fear.

So these two things together, I'm coming in telling people this template must be here, and if you don't do it, everything's going to be completely destroyed. And last time I checked these companies been operating a very long time and they've been making money before we came. Do they need us? Of course.

And can we make a lot of value? Yes. However, we can't go in there thinking that we know it all, and these people, are oblivious to, to managing risk.

[00:18:36] **G Mark Hardy:** Yeah, and, and you mentioned fear. Of course, there's, it's the fear, uncertainty, and doubt, the FUD that we used to talk about, and I remember back well in the eighties, that was kind of how we sold security because we hadn't really figured out a good business approach. And so you come in here and if you don't do this, Everything horrible will happen.

Okay. your CC mail server will go down, your fax machines will stop working. Whatever it happened to be back then. But what we [00:19:00] found out, and this is my observation, is that although you could increase the FUD, the executives had an antidote for it and it was denial. Oh, this could go wrong. Yeah. But not in our industry.

Well, this, it happened over in our industry. Yeah. But not in our state, in our company and things like that. And I liken executives confronting foot on cybersecurity to teenagers, confronting the dangers of, well, drunk driving well can happen to me. I'm 16 years old. I'm, I'm, I live forever. Well, yeah, but it's the leading cause of death.

Accidents under age. Yeah. But not here, not me. Until it does happen to somebody, you know. and you, unfortunately, a lot of organizations and a lot of executives, tend to be reactive. They have to wait for something to go horribly wrong because you end up with these awkward discussions when someone wants to be that way.

They say, well, Branden, last year I gave you 1 million for cybersecurity and nothing happened. Why should we give you more? because nothing happened. That's a good thing. [00:20:00] But how do we articulate a response to something like that a little bit more meaningfully so they realize that yeah, these investments are working.

[00:20:07] **Branden Newman:** Yeah, cost avoidance is a very hard thing to argue in, in almost all business cases. you can argue as much as you want, but there's no real ROI to actually, measure. There's the absence, of something, right? The absence of something super hard to measure. I like to, , wherever possible. To our earlier point of competitive advantage and things like this, wherever possible, I like to mix in high as percentages I can of enabling functions in the company.

So say for example, you're going passwordless, say for example, you can, You can come up with a way to meet, compliance requirements that your competitors haven't figured out yet. Very creative ways to let your company go

faster or take additional risk. I think a big part of our job is allowing the company to take additional risk.

And if you can start framing things in, in this way, instead of always crying wolf and saying, if you don't listen to me or give me more money, or do. everything's going to go [00:21:00] bad. You can instead say, I'm going to let you go faster. I'm going to give you in a competitive advantage. I'm going to let you take more risks that you're not willing to take today because you're a little bit afraid.

What if I make this area , low risk is possible and you can start taking a little edge case risks that will let you try out new innovations in a way that can give you a competitive advantage.

[00:21:21] **G Mark Hardy:** And I think there's excellent advice and hopefully people remember that but when you're looking at CISO, sometimes we make mistakes. I mean, we all make mistakes and things such as that. So I think you'd alluded it to it before, but let's call it out.

What is it that CISOs screw up when they're communicating with executives that breaks the communications?

[00:21:39] **Branden Newman:** I think it comes back to, to what I was saying earlier about using technical speak or using kind of these, , these theoretical based approaches instead of speaking in their language with the company knowledge that you have about how they operate and how you're going to help them move forward. We, we usually talk too much tech speak, [00:22:00] and we cry wolf Too much spread, too much FUD.

So we're, we're always just trying to do that over and over. It's really repetitive and I've seen it in many, many different industries, across many CISOs. I don't really understand why we continue to do this in the industry.

[00:22:15] **G Mark Hardy:** Yeah, I think it's just kind of a, either a lack of experience or people just want to go ahead and put their finger in the electric socket again to see what happens. , it's the old, Hey, hold my beer, watch this. You know, someone's going to get hurt pretty soon if they do that. And as CISOs, we shouldn't be doing stuff like that.

But one of the things I have seen that's effective for CISOs, particularly in relating to executives, Is telling stories, and if you're good at a storytelling, then you can communicate pretty well to folks because you're able to now package things up in a non-technical jargony way, but you're more engaging in 'em.

So any thoughts in terms of good stories that work with executives or approaches for that?

[00:22:54] **Branden Newman:** So I would say in, in individual cases, I use, , various stories to generally [00:23:00] talk to anybody that's not a. A technical or cybersecurity practitioner, so you'll, you'll use, you know, analogies I think go very well when you're talking about, , , things like cars and seat belts and airbags, you know, a lot of these types of things.

I really like the aviation industry using examples through history of how they've, how they. It took a long time through many accidents and everything to build these safety protocols and everything in, but now if you look there, you will see double, triple checks and it's really institutionalized into absolutely every, , part of the aviation industry.

So I use a lot of analogies, but. That's for usually specific examples. While I'm explaining technical issues, generally speaking, I like to use the, business cases that are established across the company already. So if you look at marketing, if you look at finance or any of the operational units, they're presenting business cases that have real ROI.

And I like to go pull those templates and use [00:24:00] exactly the same business cases when I'm, I'm presenting, cybersecurity use cases so that I'm speaking their language again, and I'm showing either ROI or avoidance of risk.

[00:24:10] **G Mark Hardy:** Yeah, so I think what your point is there is that the stories. Particularly if they pertain to the organization themselves. They're not far-fetched. They're not Well, well let me tell you about a company like us and a galaxy far, far away that didn't invest in cybersecurity. Yeah, that doesn't work. But if we can talk about things that are either directly in our organization, you said the business cases or take a look at the industry, , now how valuable is it to try to draw lessons learned from, if you will, a another organization that's in your line of work that had a security issue, is there value in that or do you think that denial kicks in and says, yeah, well, they're a bunch of idiots, but we're no idiots, so we don't care about.

[00:24:49] **Branden Newman:** , it really depends on your board and the, and the various executives, because some are receptive to this. oftentimes boards will actually reach out, right? As soon as something happens in your industry that hits some other company. they'll reach out [00:25:00] and immediately say, Hey, are we prone to this exact same thing?

So that's a good way to, to kind of get your foot in the door and start talking to them about, about various things. But, I generally use, the business cases or examples in history that, that are not necessarily showing fear, you know, driving this whole fear example, unless they've come to me.

[00:25:23] **G Mark Hardy:** Yeah, it was interesting. We just got an email, actually I didn't get it. It was our, our CEO got an email and it was from a known associate from another company that we're looking at, and there's just something about it that didn't look right and , so he said, he said, I don't know about this. You take a look at it.

And as it turned out that that other company, they had had their registrar records hacked, at which point, the attackers pointed the MX records someplace else, and were able to come up with d a DKM and SPF that all matched because they controlled the horizontal and they controlled the vertical. [00:26:00] Well, first of all, I'm really impressed.

Our, our CEO was like, this doesn't look right. And he asked us to help out because we built a lot of credibility over the years. And of course, The next question was, can this happen to us? And I said, well, basically we've got MFA on everything and we control this and that can't happen. And the only way that could happen is if your two security guys both get socially engineered and we both get popped.

And he said, I feel good about that because we've built that confidence. So I, in fact, I even forgotten that explanation when I was talking about MX records and things like that, that the CEO was actually on the CC list, but he responded back to that and he said, great. So the explanations you give, even if they're technical, they could be written in a way where they're not so geeky.

That, you know, is the kind of the, , joke goes. It's so simple. Even executive could understand it. And it's, it's, you know, we are in the executive suite so we have to represent that these are our peers and things [00:27:00] like that. Um, now that's great for the storytelling and communicating and, and I absolutely agree with you there.

But how about on the other side, practicing. Good listening skills because obviously we need to ask questions of the executives to make sure that they can voice their concerns and if they can champion our goals and things like that, that's even more likely that we're going to be successful. But are there any questions that you find that are helpful to bring up a thoughtful discussions with business executives?

[00:27:28] **Branden Newman:** I think you'd be very surprised at how much insight you can get from just listening to the various executives across the company. So many CISOs for one, just don't get around enough. Especially in very large companies, they'll get so inundated with all these new problems that they inherit and start trying to fix all the technical issues and processes, et cetera, that they don't really get out enough, if you will.

So that's the first thing. Definitely get out, spread, spread among all the executives, get to know them, but when [00:28:00] you're talking to them, don't, don't just come to them with, I'm going to do this and I'm going to do that, and I'm here to help you. Really give them open-ended questions. I, I'm amazed at what I learn when I go to people that have worked in the company for a very long time, and I say, I'm here to help.

From your perspective, what would you say the biggest issues are for cybersecurity in the company? What, what's the data that's most important to you? What do you think drives this company? And they will come up with insights that are very, very interesting about things they've learned over working in the company for a very long time, or areas that you didn't get from reviewing the mission statement, the financial statements and everything so far.

And it's, it's really insightful I would say.

[00:28:41] **G Mark Hardy:** Yeah, there's a lot that's in writing, but there's a lot of what we used to call tribal custom. I dunno if you're still allowed to use that term anymore, but it basically means unwritten rules where it's not part of any formality, but it definitely happens and if you come in to a C-suite, let's say [00:29:00] you've worked your way up or even come in higher from the outside, it's the matters you said of figuring out where the money's coming from, what is the moneymaking elements. Where's the reputation risks that are out there? How do we protect that? How do we go ahead and engage with the executives to allow them to explain their concerns, their perception of risks? Because at the end of the day, I like to say, and I've said this more than once, our job as cybersecurity leaders is to ensure that our executives make informed risk based decisions.

It doesn't mean they have to agree with us, and they could still say, yeah, I want to drive around at 90 miles an hour on the ice with no seatbelt. And you could say, well, you're risk informed and you know that that's a bad idea. But at the same time, I think you'll find out that if you can articulate. The position of why this is not good for the organization.

Utilize the stories, as you had said. Pick something that, that you know, that other people can relate to. I'm okay. I'm a private pilot, didn't fly rotary, but I did fly fix wing. So you [00:30:00] understand everything there is on checklists. In fact, there's a great book back here somewhere called the Checklist Manifesto where, a guy, if he hadn't read it, the guy looked at it and he started there.

But he looked at medical procedures and hospitals had started using checklists actually, Decreased their mortality because things didn't get forgotten. Now, every time you go out and pre-flight an aircraft and you hop into cockpit, you don't just, oh yeah, I've been doing this a hundred times. I remember it.

You take out the checklist, you've been doing it for 50 years. You take out the checklist. And so for us as security executives, what we're doing is we're sort of building our own. Checklist, how to go ahead, get our budgets, how to go ahead and understand risk, how to get champions out there. , in fact, how is a good way to identify somebody who might be able to, to bat above where you are in terms of political influence to become your champion and help you push any, any insights on that?

[00:30:54] **Branden Newman:** I think it goes back to building the trust in a way that you enabled [00:31:00] them. To do something. So when I go find, for example, a property president somewhere in my company today, if I solve a problem for them or I take better, even I take one of those insights from the very first time I met them where they've observed something and I go fix it and come back, circle back to them and say, Hey, that one thing that you said when we met was x and we went and implemented this thing to make your life a lot easier. Once you can get that trust built by, by enabling them on some topic, then they will become a champion for life in my experience. Because they say, Hey, this person came in, put their money where their mouth was really delivered for me. And I, I think that the, you know, their quality and I will champion them from here on out.

And that goes a very long way.

[00:31:47] **G Mark Hardy:** so it's really a cumulative virtue, if you will, that over time you get little wins and maybe some big wins here and there, and as long as you got a really good batting average and don't screw up big time. It sounds like these [00:32:00] relationships build out. And then finally, someone says, Branden thinks this is important, and he's been right all along.

Let's go ahead and give him more resources to get this thing done.

[00:32:10] **Branden Newman:** Yeah. And save your, save your cards for when it really matters. I mean, when you start crying wolf all the time, they're not going to listen to you. Right? So I, I really only have few times in a year that I'll ever raise a flag. That's significant enough to go up to the C-suite, for example, solve the things you can, don't overestimate risks and really save the times that you're going to actually ask for something that's very significant because then they'll listen.

[00:32:38] **G Mark Hardy:** That's, that's a good point. Now, with respect to references and things there, any books or classes or conferences or forums that you could recommend that CISO's leverage to learn more about either building a strategy or, or being able to do effective influence?

[00:32:55] **Branden Newman:** Sure. So, I read a lot of books in cyber. I I listen to a lot of [00:33:00] podcasts, like this one for example. and I go to whatever conferences my schedule allow during the year. I, I don't want to particularly, , plug individual ones cause I know I'll miss some very good ones. but my favorite thing is, building a network of trust, trusted CISOs either in your local area or virtually, that you can kind of have this place that is not inside of your company.

There's no kind of backlash for what you say in there and such where you can really start talking about everything from strategies to issues you're having, where you're running up against, resistance in your company or even technologies. That's really my favorite, is to get into one of these Slack groups or CISO networks that you can, just toss ideas around and just be completely informal with this group that thinks a lot like you and has a lot of the same things that keep them up at night.

That's where I really get a lot of insight. And then you don't have to listen to all the podcasts. You can just listen to half of them and, , get the rest from that group, as you're [00:34:00] tossing ideas around.

[00:34:01] **G Mark Hardy:** Yeah, or depending upon the cadence and the diction of the podcaster, you can sometimes play a 2X and not miss anything.

[00:34:08] **Branden Newman:** Oh, that's,

[00:34:09] **G Mark Hardy:** so that's one of the things I've tried over time is to make my cadence such that if you could play this at 1.5 or 2X, you can still understand all of it. And that's a tough challenge, but it can be done.

And so far, so good. There's a couple other podcasts I listen to at 1.5 or 1.75, and I know my partner here, he, he listens to everything at 2X and so he consumes a vast amount of podcasts every week. So it becomes a huge, huge wealth of knowledge. And it's like, where do you learn all these things? He says, well, the more you expose yourself to learning, The better you're going to do.

And again, you know, it comes back to what I've put out over 20 years ago, and you probably heard it, maybe not, you know, G Mark's law half of what you know about security will be obsolete in 18 months because the rate of change is just so, so fast. And for anybody who wants to get into cybersecurity and do well, they have to be able to do that.

But for CISOs, particularly if you want to be a world [00:35:00] class CISO, there's some things other than just grinding it out or being good or understanding the finances or the politics or whatever. Is there anything that you think of as like a secret sauce to becoming a world class CISO?

[00:35:13] **Branden Newman:** I, I think that being pragmatic is the number one thing that CISOs can do. So have a personality that makes you a real person in the company that they actually want to talk to and, and, and know and be pragmatic about what's going on. So, again, don't take it on full theory, don't come just with your controls and say, I'm, my job here is to put in all these controls at the company.

Come in there, understand the company. And just like you said earlier, our job's not to protect the company. Our job is to educate the leaders of the company in yet another subject that they have many, many that they need to be educated on so that they can make an intelligent risk decisions.

[00:35:57] **G Mark Hardy:** and I think that's, that's great way to [00:36:00] kind of summarize things. Is there any other departing thoughts that you'd like to.

[00:36:06] **Branden Newman:** No,

[00:36:08] **G Mark Hardy:** I mean, I think you covered, we covered a lot of ground. This has been awesome. And so, yeah, you're probably getting tired to us late in the day. But, Branden, I can't thank you enough for coming on the show and, and thank you for sharing your thoughts, your insights, and your, your words of wisdom on, on CISO Tradecraft.

[00:36:22] **Branden Newman:** Thanks for having me.

[00:36:23] **G Mark Hardy:** And for our listeners, we appreciate you spending your time with our show this week. And if you've joined our show, if you can't, give us a five-star review and make sure you subscribe to the podcast. Now, if you like video formats, try our YouTube page and please follow us there. We're trying to get our followers up and if you like to see our smiling faces, you can do YouTube or just turn on the volume in. But in addition to the podcast, we're trying to reach you as many ways as we can, and if you'd like to get into the discussion. Follow us on LinkedIn and give some comments there. We put a lot more out there than just the podcast. This is your co-host, G Mark Hardy. Thank you for very much for being a part of CISO Tradecraft this week.

Until next time, stay safe out there.