#205 - Wisdom from the 1st Cyber Colonel

[00:00:00] **G Mark Hardy:** Today I've got an army colonel, retired, who was the very first cyber colonel in the United States Army, who's gonna share with us his insights on leadership, some of his rules for how to live by, and secrets to success that have been very helpful for many people in their career.

Also, I'd like to invite all of our listeners and watchers to come out and join me on CruiseCon 2025. That'll be from the 8th to the 13th of February this coming year out of Port Canaveral, Florida. Hey, a cybersecurity cruise ship. What a brilliant idea. you can be part of that. And if you go to CruiseCon.Com you can go ahead and if you register with the CISOTRADECRAFT10 code, you'll get 10 percent off.

Come join me at CruiseCon this year and I'll look forward to seeing you.

[00:00:46] **G Mark Hardy:** Hello and welcome to [00:01:00] another episode of CISO Tradecraft, the podcast to provide you with the information, knowledge, and wisdom to be a more effective cybersecurity leader. My name is G Mark Hardy. I'm your host for today. And I've got a very special guest that I am sure you're going to be fascinated with, Mr.

J. C. Vega. Welcome Army Colonel, retired. We have worked together actually on his world that he has created some amazing resources out there for security professionals. But I'm going to let him tell you a little bit more about himself. But first of all, JC, welcome to the show.

[00:01:31] **JC Vega:** thanks, G Mark. Glad to be here, especially with your audience. I've been a fan of yours for many years, and I know we've been in the community. Quite some time, but I actually, we didn't meet until later on in the years. So being able to work with you now, it's just been a pleasure for me.

So if I sound a little fanboy ish, it's because it's true.

And

[00:01:55] **G Mark Hardy:** JC has created something called Wee Dram and I'll let you put a [00:02:00] plug in for that. And what I found that fascinating was it is a weekly call. Where, unlike our podcast, where we go ahead and we do a ton of research and we write everything up and then we do an episode and push it out, yours is live every week.

And it allows people to not only contribute their ideas, but interact with some really amazing speakers. And you're able to continually get a group. I want to tell a little bit, folks about Wee Dram and if perhaps they may even be eligible.

[00:02:29] **JC Vega:** sure. So first, let me give you a quick background. Why, how the Wee Dram ever came about. I'm a cyber guy. I've been doing cyber before cyber was cyber. And, one of the main things that came about from my career was building the cyber community, actually creating the discipline that is cyber.

Officially, I'm the first cyber colonel ever in the United States Army, because we created this concept of what it is to be community and what it is to be a [00:03:00] discipline. with guiding principles that bring the community together. So bringing the community together is something that has been continuous throughout my career, bringing it to cyber.

COVID hits and everyone now is remote. So a few of us decided to, let's get our friends, our colleagues, the people that we would meet at a conference in the hallway. After a great presentation and then talk about the presentation, critique it. What's good about it? What's bad about it? What's its shortcoming?

And we decided to bring that all together on a weekly format. We've been doing it for over four years now. How do you become eligible? You got to be invited by one of the members. And so that's the litmus test. If they want you in there, then you get invited. It's reserved for national and cybersecurity executives where we can talk shop without a business development.

What does that mean? We get to talk about the [00:04:00] issues that matter to us at that moment in time or things that we're forecasting out. And I get to bounce ideas. against peers without the fear of being judged or sharing some intellectual property or something. This is a trusted community. And if you would have told me how to build this, I would have given you some principles how to keep it going for over four years with Anywhere from 150 people at a time to, 50, it's, the community that keeps it going.

And so it's, quite an interesting format and, discussion.

[00:04:39] **G Mark Hardy:** It is, and I've been privileged to be a member. So for any of our listeners that have reached out to us in CISO Tradecraft, and we've exchanged communications and something you might want to add to your portfolio, send me a note or drop me a line. And if it makes sense, I'll go ahead and endorse you. But oh, by the way, you might need one of these.

Stand by. Let's see. [00:05:00] It's called Wee Dram for a reason, and it usually involves having some sort of a libation. This is a very particular one from one of your Attendees, Scott Sanders, he was also a classmate of mine who went on as he retired as a two star admiral to go ahead and make bourbon at Tobacco Barn Distillery.

And this was his very special batch of 700 mile an hour bourbon where he got together with his buddy Art Knowles. And, comes in a helmet bag, too. It's got its own challenge coin. And, a patch for 700 mile an hour bourbon. And, so what happens is, that there are certain things that you could mention, which I may have done so in passing, but I'm not going to give away the farm here, that could, require some partaking of something.

And it can be just like a glass of water, which I normally use. but that's something a little bit of fun to there. So I set [00:06:00] that there is a little bit of a Easter egg for people to think about.

[00:06:04] **JC Vega:** That's absolutely right. We say we talk about serious subjects, but we don't take ourselves seriously. It's after hours and it's intended to be a light conversation. Again, we try to mimic, you just heard a great presentation and now you belly up to the bar or in the lobby. And you talk about it among your friends, and that usually involves partaking in some type of beverage.

So we have a little Easter eggs in there on when the beverage partaking takes place, when certain key words come up, and we don't, you'll know it when you hear it, because you'll see everybody taking a swig of whatever they're drinking.

[00:06:43] **G Mark Hardy:** It's a lot of fun. And the thing I like about the format too, is that you'll go ahead and you won't have a German talk for 45 minutes. Rather, it's a nice brief presentation, just about the size of a TED Talk. Now, TED Talks are limited to 18 and a half minutes. Here's about 15. And kicks off the [00:07:00] conversation and it's respectful.

It's not like one of these, internet troll chat rooms where people are insulting each other back and forth. It's, some really amazing minds there up to and

including four star generals that are retired. And, yeah, it's a really great group that you've put together. And I have a tremendous.

Respect for what you've created for the community.

[00:07:22] **JC Vega:** And I'll tell you just one last plug on that. It is not groupthink. We, you are invited to share ideas that are counterculture, that contrarian view, because if you don't hear it from us, who's going to tell you when you're back with, your own organization where you are the senior person and you come up with this crazy idea and no one is going to tell you the emperor has no clothes.

And so the idea is that it's a, I wouldn't call it a safe space, It's a place where you can go in there and have a discussion, contrarian [00:08:00] ideas to certain things. As long as you're respectful, the conversation will continue. And we've talked about some very interesting things that Forget the politics of this that are extremes on belief systems from a cyber security perspective, to constitutional perspectives, but things that are relevant to our discipline.

[00:08:23] **G Mark Hardy:** And remind everybody that, if you do choose to participate and again, contact me, if there's something of interest to you, that's Chatham House Rules. And that's an old tradition back in the UK. that said what? What says, what's said here stays here. It's like Vegas in a way, but the idea is that, or you should be able to feel free to speak openly and not have somebody come back and haunt you saying, I heard you this, or you find yourself quoted in the press.

It's absolutely off limits for what we do. And everybody has abided by that now for quite a few years, which is where the trust comes [00:09:00] in, creating a community.

[00:09:01] **JC Vega:** Three rules. Chatham House rule is one. The other is, no business development, don't sell to me. And the third is be respectful. Don't be a jerk.

[00:09:11] **G Mark Hardy:** Pretty straightforward. Now, your background and my background had a lot of similarities in the fact that we were both privileged to serve our nation and wear the cloth of our nation as military officers. You retired as an army colonel, I retired as a navy captain, and you had a chance, you said, to be the first army cyber captain colonel I'm sorry, I'm gonna get the ranks straight here.

In the Air Force, we, call you a Colonel. I said, no, in the Air Force, you'd be calling me Major General, but enough of that. And we, we always have these little poking things and we poke at each other. But because of your career experience and your leadership and leading and building teams like that, you've come up with a number of thoughts about mission command principles and things such as that, which for those of us who have served in [00:10:00] uniform, a lot of these would be, Pretty much self evident, but for those who may not have served in uniform, let's translate some of that into civilian speak, so to speak.

What do you think about that?

[00:10:10] **JC Vega:** No, that's great. a lot of the things that we do, we, talk about how the military does things. The military is not anything that is super special. If you have some super duper secret knowledge on how to be a great leader, because there's plenty of great leaders and there's plenty of examples that we don't want to follow.

What we do have is we have a ultra large organization that has to function. through adversity, through constant change in personnel, in hostile environments where the enemy or the threat gets a vote in the outcome of the situation. And because of that, we call it the centralized planning, but [00:11:00] decentralized execution, we have found that because of the way we operate, the way the military operates, this is Army, Navy, Air Force, and Marines.

and Coast Guard and Space Force is that you have to be able to push these principles down to very junior leaders and that's one big distinction that I would make from the business school side to The military training on leadership. In business school, you have great examples. The North Star, the principles of the North Star.

You have Harvard Business School that, and multiple business schools that you can go to. Wharton that will prepare you to be a great business leader. But oftentimes, the connection between that individual and the organization and the rank and file is often quite a big gap. Mission command brings [00:12:00] it down to the lowest level within the organization.

[00:12:05] **G Mark Hardy:** So if we think of that, and being able to bring it down, that has a lot to do with team building, because it's not just simply, let's round up all of our junior executives, our junior officers, in the same room, and then we're going to give them their, here's 50 CCs of leadership, that'll last you a couple weeks, there you go, get out there, and do your thing.

So how is that better done in terms of building out teams? What are some of the baseline requirements for that?

[00:12:31] **JC Vega:** when you think about when you're building the team, first of all, it's based on a one basic fundamental of trust. And when we're talking about building communities, That is something that is fundamental to any organization. If you don't have trust in the people, the leaders, the process, or belief in its vision, then everything else will [00:13:00] be second guessed from there.

And so the idea to have this shared understanding. So I'll quickly just list the principles so that we can cover them in any order. Building, cohesive teams is, one of the fundamental things. The other is to have a shared understanding among the organization. That means everybody has this, the same understanding of the mission, the situation and each other's roles, duties, and responsibilities.

You also have provide, and this is a major thing. We call it commander's intent, leader's intent, but that is a clear understanding of what defines success for the organization. That is not a who, what, where, when, why. Okay. that's a why statement. This is why we're doing it, and this is the end statement.

If you get to Simon Sinek, if you're a fan of him, focus on the why. It's more [00:14:00] focused on the why than on the how. Then you have the idea of exercise discipline. That means a lot of different things, is you have duties and responsibilities and authorities. We expect you to act within that. Within that realm, within do your job.

Don't do my job. Do your job and do your job to the best of your ability. The other is have clear directives. We call those in the military mission orders. It could be policies. It could be procedures, but make sure they're clear and understood throughout the organization. And the last one is As a leader in an organization, you accept prudent risk.

That means that you, failure is a possibility and you try to reduce the, impact of failure. But if you're in a no fail situation, a zero tolerance situation, we've tried that. And what that does, it takes away initiative. It takes away innovation. [00:15:00] No one is willing to step outside of the, of, the go trail to do anything that might bring improvement.

Because if it doesn't, you fail. And if you have any tolerance for that, then you have no tolerance for innovation.

[00:15:18] **G Mark Hardy:** Some very good insights. So let me pick apart a couple of these ideas that you've suggested. You talked about building cohesive teams and having that based on mutual trust. Now, if I am a CISO or inspiring a leadership role. I pretty much understand, because I've worked my way up organizations, whether or not you trust the boss, and you can tell pretty quickly whether somebody is congruent with their actions and what they say or not.

How do I build that trust with my people? I can't just go out there Aladdin and say, do you trust me? how do we do that?

[00:15:53] **JC Vega:** I'll tell you that actions speak louder than words in this case here. So if [00:16:00] None of these principles, these six, act independent of one another. for instance, if I give you the leeway, or the initiative, I empower you to do something, and you fail, are you going to get reprimanded? Are you going to lose your job?

Is it going to cost you something? You stayed within the prudent risk, and you stayed within my commander's intent, my leader's intent. I asked you, or I expected you, to do this, to achieve this. And you did it, but you might have strayed on the borderline of some of these things, or you may not have achieved it.

Am I going to punish you for failing or am I going to double down on you and invest and say, okay, I see your shortcomings. I see where you were off target here. Let's readjust. Let's recalibrate. Let's talk about this. And [00:17:00] then as a team, how do we go forward from here? Building that team is more than just the individual that we focus on right now, especially in cybersecurity.

I think of it as you're building a championship team, a Super Bowl caliber team. what does that mean? That means that I only need one quarterback. I only need perhaps one star wide receiver and a secondary and a tight end and then go down all the positions and I need you to be the best at your position.

As I'm building these teams. I'm not expecting the defensive back or wide receiver to be the quarterback. I expect them to have some understanding of how all that works, but I need them to be the best that I can. That best that they can be. In that, if I see shortcomings, I build on that. On that need that I have for the organization, but let's just [00:18:00] say, for instance, you have a, you're challenged with working with people, there's introverts and extroverts, and there's those who handle it well, one way or the other, and then there's those who don't, and if you're one of those individuals who prefers to work alone,

head down, why would I put you in an environment where it's a communal working space, that is going to cause you frustration.

Instead, let me make, let me help you create the conditions for you to be the superstar at your position. And the idea is I'm investing in each and every one of those team members. And they see that investment. And if, they're lacking in something that there's enough communication, there's enough understanding of what our mission is, that they can bring it up to say, I could, [00:19:00] I would better serve the mission.

If I had this skill or was able to do this or focus less on this and more on that. And the idea is that you're building this championship team among, given the skills that you have and using, the term we've heard plenty of times said is you don't go to war with the army you want. You go to the war with the one you have.

In this case here, it's the, it's true in cybersecurity and there's an incident. You're going to fight this incident with the team you have, but everything before that, you have the ability to build that team, to shape that team. And you're looking out for not just the best interest of the mission of the organization and the team.

You're also looking out for the individual. So if they stray, if they falter, it gets identified and it gets, addressed and fixed. But again, the [00:20:00] idea of they have the confidence that you're looking out for them and They're looking out for you. It's mutual trust. It's not one way trust.

[00:20:09] **G Mark Hardy:** Yeah, and I think that as you talk, we, I mentioned a couple of weeks ago on my episode when I was talking that one of the secrets to success in command is knowing when it's okay to fail. And we talked about that a little bit offline and it's exactly what you were saying here is that. And what you said was a little bit different than my cultural experience in the Navy.

And so you talked about how in the Army, how you're creating opportunities for your junior officers, for your people, to fail. Not because you're being mean to them, but you're trying to give them an opportunity to work through the problem set to be able to gain that self confidence for when they finally get it.

Could you elaborate a little bit more on that?

[00:20:50] **JC Vega:** Sure. So talk about the process. Formally, for a junior officer, say someone who's just out of college, has this [00:21:00] job for the first time within the first year, What the army will do is they'll mask your rating.

What does that mean is that they'll cover it up They're saying ever your boss said about you will not be visible to for your next promotion That is so that your boss can give you candid honest feedback on where you could improve Then the next one comes.

You already had this developmental period. Now it counts. Now it's gonna stick with you. And so the idea is that I can tell you candidly, here's where you're doing really well, here's where you need improvement, and here's where you genuinely suck. And As a manager, am I going to put you in environments where you suck?

Where you're going to have a propensity to failure, to fail, or am I going to put you in the other environments where you're [00:22:00] more likely to succeed? So now I'm picking roles and responsibilities for you that align with your attributes, that align to things that you can do really well. Now there's a fundamental there.

The fundamentals, everybody has to know it to some level. And we see it all the time. We call it the, emergent leader. When you put a group of people together, someone is going to emerge a leader. I don't care if it's kids trick or treating a group of people that meet on the beach or people at a party, you're going to see this dynamic play out. I say my own experience is don't fight that. Just observe it, see where it lands. And now you start to see how you're going to build these teams around these different personalities. And when you're hiring somebody in cybersecurity, one of the major things that you have to look for is how are they going to fit with your team?

using the sports analogy [00:23:00] again, you had great football players who were only great when they changed teams. It may not have been the performance of the individual. It might've been the environment they were in. It doesn't make one better than the other. It just means it wasn't a good fit.

[00:23:18] **G Mark Hardy:** And that's key because as leaders, it's our role to ensure that we are putting our people in those right slots. And sometimes they start out wrong. They get assigned to us, said, Hey, here's your new, Fill in the blank, this particular role. And if we take the time to observe their performance, provide them with the feedback and realize, Hey, they may actually do better over here.

you can move the chess pieces around. You've, got that ability. this is not something that says, I'm sorry, this is a union rules that say, I'm not allowed to do this. I can only do that. Now that may exist someplace, but pretty much not

in our careers, but more importantly, what allows us then is it shows our people that we're involved in there.

We're paying attention [00:24:00] to it, but at the same time, as you had indicated previously about somebody who may tend toward being an introvert. At some point in time, we go through these four different phases of our careers, and I've discussed these a number of times. The technical, the management, the leadership, and the political, to get to the point.

The stars. And quite honestly, not everybody keeps going, and maybe not everybody should keep going, because that's called the Peter Principle, when you get promoted to your own level of incompetency, but they can't demote you because it's against the culture of the organization, so just leave you where you're bad.

And part of our wisdom is to find out where people, if you will, top out, and allow them to persist there. What we would have in the equivalent of a warrant officer program, where you stay in that line of work, and you don't, Oh, try one of these, try one of these, try one of these, try one of these in that career type of progression.

But going from that, another point that you had talked about was understanding or creating a shared understanding. Everybody ought to understand the mission, the situation, the roles, as well as what you [00:25:00] had called the commander's intent. Can you talk a little bit more about how do we get that word out and then how do we make sure everybody knows exactly what you plan to do as a boss?

[00:25:08] **JC Vega:** Sure. So first of all, let's cover the idea of shared understanding. What is the purpose of why are we here as a cybersecurity team? And oftentimes what I see with junior people is I am here to protect against X threat. I am here to make sure that if I'm the CIO or work for the CIO team, I'm in here, I'm here to make sure the green light is on so we can communicate.

That is not your purpose. Your purpose there is to enable the business to do whatever it does is to enable the operation.

[00:25:49] **G Mark Hardy:** huh.

[00:25:49] **JC Vega:** it may be from a cybersecurity perspective. It may be to do it securely, to do it at less risk. To do it within the parameters of [00:26:00] whatever it is that the organization is there for.

if you look at, let's say, a university, what is it, what is its core mission? to the student, Core mission is to get a degree. That's for the student. For the tenure track person, it may be to publish research. And you have all these different ideas, but understand that shared understanding of you have different motivations for this, but you have this coming together of These different ideas, these different concepts for an end state, a goal.

And that gets to commander's intent. What is commander's intent? when I have a group of, a diverse group of different levels of leadership, I give them a real simple example of being at home. [00:27:00] And if you're a parent, have kids. Or all of us were a kid at one point. This is what I mean by having this clear understanding of what defines success.

You, the scenario is you're leaving for work in the morning. You're going to come back and you're going to cook dinner and you're going to have a you're going to entertain that evening. So that's a scenario you have as the parent. And so you have two options in this extreme example of you tell each of your subordinates, in this case, your kids, I need you, I have a list of things you want to accomplish.

You need to accomplish. I need you to do the dishes. I need you to vacuum. I need you to do all these different tasks and they're all very specific to the age. You know who the leader is, who the eldest is, and you know who's going to be better at doing something and you divide this all out, regardless of age.

Everyone has a very specific role. This is your organization, whether it's HR, whether it's, [00:28:00] the CFO, whether it's a COO, whether it's business development, you all have a role in this success. of the organization and its commander's intent in the end state of success. So you come back home that evening and you realize that they did exactly what you directed them to do and not a single thing more.

And they're going to fall on that sword. I told you exactly, you told me what to do. I did it. Why are you disappointed? I'm like, I told you to fold the clothes, but that also implied putting it away, not just

[00:28:39] **G Mark Hardy:** of the ten talents, right? Buried mine in the ground so you could have it back.

[00:28:45] **JC Vega:** You did the dishes, but you left them all drying on the counter. So you didn't quite get that end state of what I meant. So, here's the alternative commander's intent. You're leaving, you get the team together and

you [00:29:00] say, I want to come back. I want to have a Zen environment. When I come, I want to be able to come home and.

Put my things, out that I'm going to cook and get ready to just start entertaining and start getting the environment set up for me to do what I have to do. That implies that these things have to be cleaned up, picked up, but I'm not going to tell you what or how to do it. So taking this back to the corporate world, if you're trying to build this organization, are you going to tell the HR person how to recruit people, how to do their job?

Are you going to tell the CFO how to manage the money? Are you going to tell the business development person how to do sales? Are you going to tell the COO how to manage the operation? Thank you Or are you going to tell them that we want to increase revenue by this much. We want to enter this market and we want to achieve these [00:30:00] goals by this time. All of this is all of your job to get us there. Anyone have any questions? Before you leave, you have the whole team there. Are there any questions? You leave, but now you have all of, your, subordinates there, the team. in this case, the kids now, is what did they mean by that? And they will have to figure that out to ensure that when you come home, you have that Zen environment.

Now, the idea is that they're going to do what it takes to achieve this vision that you described as the end state, the success. And you don't have to tell them how to do it because back to the corporate world, they're experts in the how to do their job. Don't do their job. Nobody wants you to do their job.

If you're doing their job, you're going to [00:31:00] hold them back because now they're going to wait for instructions on how do you want me to hire? Because I'm not going to lean too far forward. If the, result is going to be, you're going to tell me how to do it anyway. And I did it wrong. And so the idea is get out there and do it.

And give them the, empower them, give them the initiative to get it done.

[00:31:20] **G Mark Hardy:** Which brings up kind of the point you were talking about, accepting prudent risk. Now, as a commander You're analyzing risk on a regular basis. In the business world, part of that risk is deciding, could this new person, this junior person, complete this task adequately? And the answer may be yes or no.

If the answer is yes, it's a good assignment. But if the answer is no, then you have another decision tree. Not just give it to somebody else, but what happens

if it doesn't succeed? Will this person be able to complete this report? It comes back, it's all marked up in red, and it's hey, try it again.

All right, and if they've got any [00:32:00] desire at all to succeed, to try to go ahead and feel good about themselves, they're going to go punch the pubs, they're going to read things, they're going to research it, they're going to, these days you just go online. Hopefully not over to ChatGPT and have it fill out for you, but the idea is what?

that you continue to get better at it until you get to that acceptable level. Anytime you're trying to learn something, you start out where you really don't know. I've been doing my Duolingo now. I just crossed 420 days of Español. And I think, I'd say, hey, let's just go over into Spanish.

Except what I found is what? My reading comprehension is way up, but my verbal isn't that great because I've had no one to speak with. And so sometimes you get people who will have a lot of training, but the training may not enable them to be immediately successful in the role for which you want them to have.

But get them in that role, get them to start speaking something. Yeah, they'll miss a word, they'll make something wrong, but give them another try and eventually it's that familiarity that gets there.

[00:32:59] **JC Vega:** And that's [00:33:00] a key thing is when you're training, developing the team, there's going to be missteps. There's going to things. And you look back, you could have done better. They could have done better. We could have done better, but the idea of accepting that prudent risk, what, does that mean in, In simple terms, what I used to tell my team, this was in the military now, is don't write a check your butt cannot cash.

Because if the risk isn't associated with something that you can handle, that is within the dollar amount, within the acceptable risk level that had been pushed down to me and then down to you, please do not put the organization at risk without informing the organization or the leaders, what that is. So how does that translate into something practical is you have [00:34:00] a certain skillset, you have a certain training, development, knowledge, skills, and ability that you're expected to do.

If I'm going to push you outside of that, or you're going to step outside of that, We have to have an understanding of this is not your forte. This is not your expertise and how much you're allowed to fail in that. And risk that I'm

accepting is something that we're going to be very upfront about. We call it guardrails, call it boundaries.

It could be a dollar amount. It could be a level of effort amount. It could be a time amount. If this task starts to take you more than 30 minutes, you need to ask for help because Time matters to us in an organization. if you're seeing something and we have an acceptable level of tolerance for mean time to detection, after that, you have to tell somebody, don't sit on that information and you have to set those boundaries, make those [00:35:00] clear.

And what that does, What you intend to do with that is within those boundaries, you're empowering your team to try innovative things, to really push the envelope on their, on within their knowledge, skill, and ability. Up to that point. Within that point, it's no longer your risk. Now it's elevates above that, and now we have to accept that.

And again, it can be defined in time, it can be defined in resources, it can be defined in dollars. Any number of things is. Don't push it outside of that. And I always tell people, don't create work for your neighbor. Don't create work for the next person. If you can't handle it within there, don't just toss it over the fence.

Is that we're in this together and there is no fence. If. If someone is on your team with that, and what does that mean is stay within your guardrails. That's that prudent risk.

[00:35:58] **G Mark Hardy:** Yeah, and it reminded [00:36:00] me of one of the lessons that I'd learned when I was training to work at the Pentagon is one of the rules is an action passed is an action completed. Which basically says if you can pawn it off on somebody else, you can write it up, check it off your list and you're good. And there's an awful lot of passing that around.

But again, a little bit too large to be thought of as, a one big team. one of the things that I loved about some of your philosophy about leadership and, people in general is your rules to live by, which you call the Vegas top three. Some of those kind of almost align exactly with what I print on the back of my business card, but I'll let you introduce them and talk a little bit about the Vega's top three.

Tell me some rules to live by.

[00:36:40] **JC Vega:** Sure. So I do a lot of mentoring, a lot of public speaking with different groups, and oftentimes they're underrepresented groups who are trying to either break into the discipline or trying something new. Or it's an organization that is, that I'm advising that is trying to break into a [00:37:00] new market or do some type of change management.

And there's a lot of rules out there in the world, a lot of rules out there. So I've narrowed it down to, this is how Vega handles. rules. Now, I have to give you the warning. You have to have some maturity within that and some emotional intelligence, some experience. You have to have a before you can exercise these rules and don't exercise these rules beyond a check that your butt can't cash.

So there's prudent risk there and there's, Exercise discipline, within that. So rule number one is don't accept no from someone who is not authorized to say yes. What does that mean? That means that imagine you're going to customer service and you're trying to Get [00:38:00] them to give you a refund or tell you to do something or get them to do something that they are not authorized to say Yes to.

The only answer they can give you is no. don't accept no from them. Take that to the next level. Think cybersecurity now. You want an exception to policy or someone wants an exception to policy because they think it's the right thing to do. It's really not a decision until, it gets to the person that is authorized to say yes or no.

There's no decision if somebody who's not authorized to say, to give you the authority to do that says, no, you can't do that. So you're going to find that in many, situations, it's easy to get that no answer. It takes some effort to get that yes answer, but the only way you're going to get that yes [00:39:00] answer is from someone who is authorized to give it.

[00:39:04] **G Mark Hardy:** So what you're saying then is don't just accept a no, because there's a whole layers out there of people who are there to say no. They're supposed to go ahead and reduce the flow up. And in fact, anybody who's ever been in sales realizes that most of your sales occur well past the first no, and usually two or three or four times into that, when you finally either get to the right person or you've reached that right level of communications.

Now, how about your second rule there? what do you have there for the Vegas top three?

[00:39:32] **JC Vega:** So this one is a little controversial in the sense of, I said, if the rules don't fit, break the rules. What does that mean? When we started the cyber career field in the Army, there was no such thing. There was no cyber career field. We had to create the rules. So we had to break the rules to create the rule.

You now, one of the, Second and third order effects of that, if you're in the federal government now, and you [00:40:00] apply for a cybersecurity job, it now states you do not need a degree, a four year degree for those jobs. That was a result of conversations we had more than a decade ago, saying there's no need today for someone to have this degree because the expertise in cybersecurity does not correlate with a degree in the field.

Not today. And so we had to put in a lot of exceptions to the policy for that. And there's a lot of great leaders among us who don't have those prerequisites. So break the rules. And this is where again, that maturity, that experience comes into play is understand why the rule is there in the first place.

So I'm a pilot. I'll take a drink to that. And [00:41:00] have a commander's intent. A commander's intent of being a pilot is to safely land the aircraft, not even safely, land the aircraft without creating any additional damage, loss of life, site or limb. And we have multiple regulations that we have to follow.

But if anything contradicts or it's going to put me in a position where I have to decide between that rule and saving the, crew and saving the passengers and getting on the ground safely as possible, I'm allowed to break those rules. Those rules are there to ensure that I'm as safe as possible, but sometimes the situation the rules don't align.

Now, there's a higher order of rules there. It has to be legal, let's say legal, ethical, and moral. If it doesn't pass that litmus test, [00:42:00] then you have some challenges. But most, rules don't get to that level. And the idea is that those rules are there to make it easier for somebody. They're there to have a predictable behavior out of somebody.

Just bringing it back to cybersecurity. I used to do network scans on our network. We didn't have a security team before. And then all of a sudden they said, you can't do network scans. He goes, but I'm actually doing security for the network. But you're now hurting the system. It's wait a minute. I'm putting a load on the system.

I understand that, but I'm also looking for threats. Which rule takes precedence here? And I had to, you had to sit there and analyze, okay, what's fundamentally, what is the purpose of these rules that we have in place? And if the rules don't fit, break the rules, but know the [00:43:00] consequences of those rules. Do not do it just because I know the rule.

Remember that part of don't cash it, don't write a check your butt can't cash. You have to know the consequences and then follow up and change the rules. Change the rules as the ultimate goal so that it applies to the situation in the future.

[00:43:22] **G Mark Hardy:** Got it. That sounds really good insight. We got just enough time for one more rule to live by. So what would that be?

[00:43:29] **JC Vega:** Don't self select out of anything. So I used to recruit for aviators and I used to go to all different universities and, talk to, individuals who wanted to be an aviator or, interested in meeting the service, not necessarily aviation. And I asked, I said, why aren't you applying for aviation?

I said, I don't have what it takes to be an aviator. what do you think it takes? I'll tell you first thing it takes is you gotta fill out the application. [00:44:00] Step one, fill out the application. Same goes for cyber security. Don't self select out. Put in for that job. Compete for that job. Make them tell you no.

And then don't accept no from someone who isn't authorized to say yes.

[00:44:16] **G Mark Hardy:** they do tie in together. I'm a graduate of the United States Army War College. And when I applied to the War College, they said, you're too senior because you have to have three years of payback. I said, I'm very happy to let you promote me to one star and pay it back. But I graduated my 30th year.

And when people said, how did you get in? I said, because I applied and the Navy had 10 slots that year. And I think only seven officers applied. They said, take them all. So what you find out then is that the rules You know, when you say break the rules, you also be careful. You have to be at a level of an authority where it makes sense.

I used to say, you'll make it to Lieutenant Colonel by following the rules. You make it to Colonel by knowing which rules to break. So don't just go in there and be like a bull in a China shop. we're pretty much out of time. I could keep going, but of [00:45:00] course, anybody who wants to hear a little bit more of

the wisdom of JC, we can go ahead and probably refer you over to the Wee Dram.

So again, feel free to reach out and connect to us here at CISO Tradecraft. And we'll be very pleased to, Forward on those that we think would make a good addition to the team. but anyway, thank you very much. this is Colonel, retired J. C. Vega, who is been our special guest today here on CISO Tradecraft.

I think this has been one of these fascinating episodes where we get to delve into concepts of leadership that transcends cybersecurity, but are built over years, in fact, decades of expertise. And you've got so much to offer the community. I thank you so much on behalf of the community for all you have done and continue to do for us.

[00:45:41] **JC Vega:** I appreciate being here with your group. And one thing I'll tell you from the difference with this, these concepts is this is not just executive level. This is an operational level. This is a tactical level. Everyone can learn from these and, happy to share with anybody. Thank you for having me.

[00:45:58] **G Mark Hardy:** You're most welcome. [00:46:00] everybody, thank you very much for being part of CISO Tradecraft. look forward to having you next week for another episode. If you're not subscribing already on YouTube, please do or give us a thumbs up or a like, or subscribe to us on your favorite podcast channel. Also, we've got a lot out there on LinkedIn that we provide during the week, as well as a Substack newsletter.

Lots of ways to go ahead and improve your CISO Tradecraft. This is your host, G. Mark Hardy. Thank you for tuning in, and until next time. Stay safe out there.