IT Matters Podcast - S1 EP 24

Thu, Mar 21, 2024 2:47PM 37:58

SUMMARY KEYWORDS

cia, cybersecurity, cyber, working, directorate, people, trust, team, ciso, call, ai, generative, air force, gen, podcast, cadet, eo, story, captures, terms

SPEAKERS

William MacMillan, Narrator, Keith Hawkey

Narrator 00:07

Welcome to the IT Matters podcast, where we explore why IT matters and matters pertaining to IT.

Keith Hawkey 00:16

Welcome to the IT Matters podcast where we interview IT leaders making an impact. Today we have a very special guest. He started his career down the path of military service to our country, first becoming a pilot for the United States Air Force and continued service in various capacities including serving as a Combat Aviation adviser to the Special Special Operations Squadron, culminating in nearly two decades of service, he finished with defending our nation against malicious cyber threats as the Chief Information Security Officer of the CIA. He now serves as an adviser to Salesforce on national security issues and as Chief Product Officer at Red Cell Partners, an incubation and investing firm focused on complementing companies changing the paradigm and the cybersecurity and artificial intelligence space. I welcome William MacMillan, welcome to the IT Matters podcast.

William MacMillan 01:17

Thanks, Keith. It's great to be here. And thank you for your very kind introduction.

Keith Hawkey 01:21

My pleasure. So you have quite the colorful and honorable background. I really want to, we're going to cover a myriad of topics today, where I'd like to start is what drew you to service? What drew you to the United States Air Force? And how did this all begin?

W William MacMillan 01:37

Yeah sure. So going way back into ancient history. I grew up in Western New York. I'm the son of two immigrants, my dad's from Scotland, my mom's from Germany. So I grew up in a household where we really thought about and appreciated what the country gave to people with very modest economic backgrounds. So as I grew up, I kind of always knew that I was going to need to do well in school and look at scholarship options and that sort of thing. I was also kind of what I guess you could call a stem kid. I was really into math and science. And that eventually led me to be selected to attend something called the summer scientific seminar at the US Air Force Academy between my junior and senior year of high school. It's really basically a recruiting event. And it's an incredible opportunity for kids across the country to be selected to go live in the cadet dorms and you know, live there on the Air Force Academy campus for a week and go to different classes and seminars. That was the first time I'd ever been on an airplane in my life was flying out there for that week in Colorado Springs. And I just fell in love with the place and I thought this is incredible. You mean I get to you know, if I'm selected to be a cadet, I can come live here and on the eastern slope of the Rampart range in the southern Rockies, you know, can live there and go to school there. So I thought it was amazing. I was super passionate about biology. So I thought maybe I would go to the Air Force Academy and study aerospace physiology, or maybe even medicine. I did apply and eventually got into the academy. Once I got there, I ended up tracking towards pilot training instead of medicine. What happened was the different Cadet squadrons, they all have these sponsor relationships with active duty Air Force units, and ours in my upper class Cadet squadron, our sponsor unit was the wing, the training wing at Kirtland Air Force Base in Albuquerque, New Mexico that is responsible for training all the combat rescue and special operations helicopter and fixed wing pilots. So I was around those guys for you know, for three years while I was an upper class cadet, and just absolutely fell in love with the idea of combat rescue and Special Ops. And, you know, so ended up tracking off into pilot training after I graduated from the academy. That's sort of the beginning of the story.

K Keith Hawkey 03:49

That's fascinating. I could certainly see the appeal as a young man and joining the Air Force and becoming a pilot. So you spent some time as a pilot for the United States Air Force, but you didn't stop there. I guess you decided that you had enough of flying and wanted to dip your toes into cybersecurity and join the operations team at at CIA. How was that transition? What led you to join the CIA after the Air Force? Yeah, certainly a different type of role.

W William MacMillan 04:22

Yeah, for sure. And it was a it was a long transition actually. I didn't jump right into cyber, but I'll explain the transition. So I was, you know, traveling around the world in the Air Force, and was in was operating in a capacity where we were advisors, which meant that we had, you know, sort of a regional expertise. And I was focused mostly on the Middle East and Central Asia. And this is, you know, back in the late 90s. So that language and cultural training and experience in that part of the world really set me up well for a transition into CIA. I was fascinated with international relations and, you know, was actually was working on a master's degree while I was still, you know, traveling around in the Air Force. And so right around the time that 911 happened, I had the opportunity to move over and join CIA. And that experience that I had developed in the Air Force with the Middle East and Central Asia in particular, was obviously, you know, fairly relevant right around the time of 911. And so I transitioned initially into being a an operations officer, you know, running intelligence operations within what's called the Directorate of operations at CIA. So it was only over time that I eventually sort of started tracking towards cyber and spent, you could probably say, the back half of my 20 year career at CIA, as a, you know, so called cyber guy.

Keith Hawkey 04:51

That's fascinating. And that's, that's when the war, you know, cyber cybersecurity, you know, warfare seems to have really picked up pace during that, that latter 10 years of your tenure, and you know, after 911 and, and beyond, I really want to get into some of the the origins of zero trust architecture, and how the CIA and your team were involved in this. But I gotta say, I've watched a lot of movies, a lot of movies about spies and the CIA, and do any, any movies portray the CIA, in a more accurate light, you know, what's the best and worst representations that you have?

William MacMillan 06:32

It's a great question. It's kind of a fun question. I don't know that I'm going to dime out any worsts. But let me let me answer it this way. You know, unfortunately, I think in my opinion, there's really no single movie that accurately captures you know, the full depth and breadth of CIA accurately. I think some movies might capture a particular aspect of the intelligence world accurately. Like, for example, a movie like Zero Dark 30, I think is generally regarded as you know, doing a decent job capturing the essence of individual dedication. But, you know, like I said, no single movie really, really captures all of it. There are some movies, some particularly some, like older school movies, like Tinker, Tailor, Soldier, Spy, that are good at capturing the cat and mouse aspects of espionage itself, the the actual intelligence operations aspect of it. But all these movies, you know, tend to fall short in various areas, in terms of the authenticity and really nailing especially the positive aspects of CIA service to the nation. You know, a development that I personally think is fantastic, is that a handful of former senior CIA officers have been working to try to bring more authenticity to Hollywood portrayals of CIA. You know, it's, it's important for Americans to know what CIA is really like. CIA relies very heavily on the talent of its workforce and authenticity is a great recruiting tool. You know, there's no more fulfilling way to serve the nation than a career in intelligence, a career at CIA. And we need talented young Americans to be aware of that and to understand the exciting opportunities there are in the intelligence world. There's, there's two guys that I'll point you towards, highly respected senior CIA leaders back in their day, named Jerry O'Shea and John Sipher. They actually started a company called Spy Craft Entertainment, specifically, expressly to try to bring more authentic spy stories to Hollywood. You can Google these guys and read about him. Another former CIA officer, a former colleague of mine, named Kari Amelung, she's somewhat famously consulted on several series like the Homeland, Homeland, The Diplomat, and, and a series called Berlin Station. And if you watch those shows, there's elements of those that you can tell clearly benefited from her involvement. You know, she's also, by the way, consulting on the upcoming season of a really big show, but I don't think it's public yet so I don't want to scoop her and get ahead of things. My point here, Keith, is that it's these, it's the human elements of spycraft that are really tough for Hollywood to get right. So it's great when they can have an experienced intelligence veteran like Kari on, on hand to you know, guide, especially to the character development in the, the interpersonal stories, and plotlines. And finally, sorry, this is a long answer. The last shout out I'd like to give, your listeners can read more about this at their leisure, a, a friend and former colleague of mine named Phil Reilly. Phil is a legendary CIA veteran, and he's worked on some documentaries like the Netflix series, Spy Ops as an advisor, and he's also working on a future series about Osama Bin Laden. I'm not sure the status of that project, so I'm not going to get into it too much. But I would just say that if any of your listeners really like the spy craft genre, and they want to learn more and follow it, they could just set a Google alert for CIA and Phil Reilly and anything that Phil's associated with, it's going to be fantastic. I mean, it's a it's a famously insular culture, right? Like by design, you know, CIA isn't really built for everybody to, you know, to get really intense insight into what it's like. So so you're right, they have they have a tough job.

K Keith Hawkey 10:14

We'll make sure to add links to those organizations and individuals in the notes section of the podcast, so look out for that anyone that's listening. So many industries are misrepresented and it's very difficult I can imagine for a producer that is looking to make something dramatic and sexy and alluring to the mass audience, to you know, because most of what I imagine the CIA does is actually fairly routine and mundane. Just like, you know, any military force, 99% of the time it's, it's doing the simple things right, often, and and with credibility, but that doesn't make for the best Hollywood movie. Blend of the two, That makes sense. Which leads me to my next question, William, is, I advise CIOs across the United States and the talk of the industry today is how they can move closer to a zero trust architecture. This story of zero trust, has its origin story partially with a team that you were a part of while working for the CIA in your CISO role. Can you shed some light on on how zero trust originated? What led you down the path of forming this this architecture and framework? What can you share?

W William MacMillan 12:02

Certainly, I can comment on on CIA's portion of the story and my role there. Zero trust architecture itself goes way back to like 2010 and a guy who was not a CIA person developed the doctrine and Google very famously worked on a bunch of that as well. I'm not really an expert and those aren't really my stories to tell. But as far as CIA goes, and you know where CIA is, in terms of its zero trust journey, and my very modest role in that, I'm happy to tell you that story. It actually involves a little bit of history. So bear with me here, I've got to, I've got to set some context in order for it to make sense. So, you know, as you and your listeners are aware of CIA played a really pivotal role in the global response to the September 11th attacks in 2001 on the US homeland, and along with our teammates in the military, the rest of the intelligence community, and the federal government at large, counterterrorism efforts very quickly consumed consumed a great deal of focus and resources at CIA, and rightly so that's exactly what the nation most needed at the time. If you think about that timeframe, like, you know, leading up to 911, basically, the technology world was really transforming. There were some huge influences, you know, you're a little younger than me here, actually a lot younger than me. And, you know, you might not, you're of the generation where, you know, if you didn't really live through the 90s as an adult, I think it's easy to lose track of just how transformative that era was. Two technologies in particular in the 90s, the web, and then also GSM Tech really exploded and started connecting the world and transforming our digital lives. And it was amazing, it was historic.

Keith Hawkey 13:57

You mentioned the web. I think everyone listening understands what you mean by introduction of the web, but you said GS4 Tech? What what was the second term?

William MacMillan 14:07

GSM, mobile, mobile phones. Went from sort of analog to a more digital format and in particular, in Europe in the 90s, right around the same timeframe as the webification of the internet. We started rolling out these digital mobile phone networks. And the cumulative effect of those two technologies was to really just connect people's digital lives in ways that had never happened before. It was an absolute sweeping change in the way that people lived. And then the dot com bust of the late 90s created kind of a lot of smoke and light that distracted everybody. But if you, you know, step back from that, as the dust settled on the dot com bust, you woke up in the early 2000s to a world that had just been completely transformed, you know, this this digital transformation that was sweeping the planet. So, what I'm setting up here, Keith, you know, to be able to tell the story in terms of context is there was a basic disconnect. The world was becoming digitally transformed, but CIA was laser focused on counterterrorism, sort of distracted if you will, even if you know only for all the right reasons. So in that context by by like the, let's call it the the 20teens, there were voices at CIA urging the organization like, hey, you know, we got to, look we're focused on on counterterrorism and that's, that's what we should be focused on, but we also have to start really thinking about this digital transformation and what that's going to mean to intelligence. We have to start transforming and harnessing this new tech. That dialogue, that that call to arms manifested eventually in the creation of a new Directorate at CIA, called the Directorate of digital innovation. Now at CIA directorates are the big pillars of the org chart. And they supply people and resources to various mission centers. These mission centers are the operational chunks of CIA that are focused on a particular region or on a particular topic. And these directorates supply them with with money, you know, long term plans, resources, people. So this brand new directorate, this Directorate of digital innovation, and what we call the DDI was fully up and running in like the 2015 timeframe. Now, when it was created, and the agency developed the blueprints, if you will, for it, IT, data and some elements of cyber, were all rolled into this new Directorate. But the decision was made during that planning period for this new directorate, that they were going to leave the cybersecurity team in the Directorate of support, which was where it had been for a long time. The Directorate of support has existed for many decades. Now, this cyber defense team, the cybersecurity team was staffed with super motivated, highly capable people. And they they coordinated extremely closely with the DDI. And, you know, as you can imagine, at CIA, you got to take cybersecurity pretty seriously. There are a ton of bad actors out there that will target CIA any way they can. Cyber is certainly no exception. But you know, with with the cybersecurity team over in one directorate, and all the other digital folks over in the new digital directorate, there was there was always a backburner discussion about whether it might make sense to move the cybersecurity team into the DDI. So that was all context so that I can answer your question. Sorry for the long explanation. But so so here we are with that context. And now I'll pause here, but I'm gonna, I'm gonna, I'm gonna answer your question about my role in in zero trust when I became CISO. All good so far?

Keith Hawkey 16:48

All good. Yeah. All good. You know, context is key.

William MacMillan 18:09

Okay. So when I became CISO, right at the very, very end of 2020, kind of officially took over right at the beginning of 2021. It was against the backdrop of really heavy nation state cyber activity in the news. So things like solar winds, and hafnium, you know, Russia, China, and everybody was suddenly very aware of, of just this dynamic, you know, hostile cyber activity going on against all manner of, you know, public and private organizations. So the new administration that was about to snap in, even before the inauguration, they kind of put the word out in the executive branch, like, Hey, we are going to be very, very serious about upping our game when it comes to cybersecurity. You know, we're going to start with the, with the executive branch, but you know, there's going to be a whole strategy. And so they were already, like I said, even before the inauguration, they'd started sort of workshopping some of the content and some of the thinking that was eventually captured in an executive order what we call an EO. In this case, it was called executive order 14028. Improving the nation's cybersecurity. That EO came out in May of 2021. That executive order told the entire executive branch to embrace zero trust architecture, among other things. But zero trust architecture, or what we call ZTA was was one of the high level guiding principles for cybersecurity practitioners in the government ecosystem. So as this was rolling out, you know, in this early period of that new administration, with with some really highly capable cyber officials and from different parts of the government, we can tell at CIA, that that was going to create a tailwind for us to capitalize on. So we looked at where we were in terms of strategy. And we decided that fully embracing this zero trust push would be good for CIA cyber defenders and would help us bring, you know, the already excellent capabilities to the next level. Now, it also became clear to us that a comprehensive push into zero trust would be easier and more effective if we repositioned the cybersecurity team into the DDI. So that team that had been left in that other directorate, we decided, we're going to move it over so that we'd have the IT teams, the data teams, and all of the cyber forces all positioned in the same part of the agency to foster closer cooperation, as we pursued a long term zero trust strategy. So at the time, when I spoke about it, I referred to a shift left strategy on an organizational scale. Shift left is a term that gets used to convey the idea of baking security into the earliest phases of IT system lifecycles. So without getting too nerdy, or getting into a level of detail that I can't really discuss publicly, that was kind of the essence of my role as the CISO was looking at the overall strategy, embracing this big push towards zero trust and, you know, being one of the players that was managing some pretty significant organizational changes, to make sure our teams were integrated in the right way. And, you know, since I've never really told this whole story like this publicly, you know, if you'll indulge me for a second, I want to give a huge shout out to the folks who were involved in that both within the Directorate of support and within the Directorate of digital innovation. You know, CIA really leaned into this transformation in a big way. And, you know, I can tell you being on the field with all these great all these great teammates during this period was, you know, honestly, it was really humbling and gratifying. And it was probably one of my favorite chapters in my career. I was excited a couple days ago to notice that people are catching on on LinkedIn, I guess it's the cats out of the bag that my, my partner, the CIO, when I was the CISO, someone who I worked with closely on a daily basis, an officer named Juliane Gallina was actually just recently fleeted up and she is now the Deputy Director for digital innovation for all of, so she's basically CIA's Chief Digital Officer, and all of these forces arrayed under her will be responsible for, you know, continuing on this zero trust journey.

K Keith Hawkey 22:37

There's certainly a lot to chew on there. The I'd like to ask about, you know, after this authorization, this EO was announced, the ripple effects must have been dramatic. I think I think it goes that if you if you are an agency, or if you're a company that wants to work with the CIA, or you know, federal entities, you now have a framework, you have a compliance that you have to abide by, that has zero trust elements inside this, you know, took the marketplace by storm. And and we're still seeing it today. And in some ways, I think organizations represent what zero trust frameworks are accurately and then there's certainly a lot of market where they like to use the buzzword because of how legitimate it is. But the the ripple effect of the announcement of this cohort strategy of the Zero Trust Architecture Framework, did CIA anticipate this to be a such a seismic shift in the cybersecurity industry? Or were you guys kind of caught by surprise?

W William MacMillan 23:53

No, I think we we did kind of see it coming because of the the seriousness of the folks that were put in charge. I mean, if you look at this timeframe that I'm describing, if you look at the cyber officials who were, you know, who were brought in to guide this strategy, you know, you had Anne Neuberger at the White House, you had a guy named Rob Joyce come back to run the Cybersecurity Directorate at NSA, you had Chris Inglis as the National Cyber Director, and Jen Easterly at CISA. Right, these are very, very serious, very highly esteemed cyber professionals. And so, you know, the table was set, and it was pretty clear that this was going to be a significant push. The folks who I think were caught a little bit off guard was there was a lot of, this is one man's opinion, by the way, so you know, agree with me or not. There was a lot of eye rolling in some corners of the executive branch industry prior to that period, about this whole idea of zero trust. You would hear a lot of people say, you know, I don't like the term, this is what this is, this is what I call cybersecurity, right. You there was there was just a lot of skepticism about the need for a term and a push like this. But when the EO came out against the backdrop of having all of these really amazing leaders in place, if you read that executive order it, you can tell that the people who put that together knew what they were doing. It's actually surprisingly prescriptive. It says, you know, embrace zero trust, embrace the cloud, you know, do better with logging all of these things. And so, what I saw happen was, I felt like, you know, and I dealt with a lot of vendors, everybody sort of snapped to and said, okay, zero trust it is. We are going to embrace this, we are going to, you know, gonna go boldly into this new future. And you're right, you hit on a, an almost comical element of this whole transition, which was that, you know, we would joke about people selling zero trust coffee mugs, and you know, everything suddenly was branded as zero trust to be consistent with this EO. But I wouldn't say that in government, we were we were surprised that people took it seriously. I think we knew that it was a serious group of people. And you know, that this was going to be a turning point for the US government where we said, okay, enough is enough, we've really got to raise the waterline on cybersecurity.

K Keith Hawkey 26:14

Yeah. And then and, you know, we certainly have seen the results of that development, you know. And switching gears here, in more recent years, in the last year, generative AI, has been the talk of the town, in 2023, 2024. This, of course, is building upon the shoulders of machine learning and artificial intelligence on algorithmic functions that are they're solving problems and data sets for a long time. But the more generative, LLM models today are far more compelling, at least to the public, than they were a year and a half ago. And I want to get your opinion, William on how does generative AI impact the offensive and defensive cybersecurity strategies and the commercial space today? Where do you see this going?

William MacMillan 27:09

Yeah, it's a great question, Keith, I'm asked about this a lot actually. There's a ton of enthusiasm for generative AI, in particular Gen AI in the cyber world right now. There's also a lot of anxiety about what it means in terms of new capabilities in the hands of bad guys. Overall, I'd say that right now a snapshot in time, there's pretty decent consensus that we see Gen AI in particular, bringing a slight advantage to defense. In other words, Gen AI favors defense a little bit more than offense. Definitely bad guys are capitalizing on Gen AI. In particular, things like phishing attacks, business email compromise, right? Like like content and language rich approaches to you know, malicious cyber activity. Those are becoming more sophisticated as a result of the language capabilities that Gen AI can bring to criminal and nation state threat actor groups. On the defense side, though, we're starting to see Gen AI harnessed in ways that are going to help the overworked and overwhelmed cyber defenders that need to operate, you know, a lot more efficiently if they're going to deal with the just oceans of data, they're generally drowning in on daily basis. This is a super, super interesting area for me, and it's definitely something to keep an eye on. So, you know, cyber is always a cat and mouse game. And for sure, in the defensive world, we need to stay on high alert about bad actors leveraging Gen AI. For now, I'm in the optimistic camp, that it's a technology that is for once sort of skewing in favor of defense teams.

Keith Hawkey 28:47

Well, that's certainly a breath of fresh air for those that are laboring in SOCS and feeling like it can be a losing battle and in a lot of ways an uphill road at minimum. But speaking of optimism, tell me about Red Cell Partners. What are you guys incubating and investing in? And I think you are a part of a an exciting project here in stealth mode. For those in the venture capital space, you will understand what that means. But can you tell me a little bit about your role at Red Cell Partners and what you're working on over there?

William MacMillan 29:28

Yeah, sure. So, Red Cell Partners is an incubation foundry. It makes startups, it's a startup factory. And it operates along the lines of three practices. So there's a healthcare practice, a national defense practice, and now our newest practice is a cyber practice that's being led by George Barnes, the recently retired deputy director from NSA. He retired last fall, and now he's running the cyber practice at at Red Cell. So so that's what Red Cell does. I am Chief Product Officer as you mentioned in a particular incubation under the cyber practice, so we're still in stealth, which means that, you know, we're not really discussing what we're working on yet, we're not really discussing our name yet, we haven't really sort of announced the whole team yet, there's not a ton that I want to discuss at the moment, we probably won't be in stealth for too too much longer. But what I can tell you for now is that I was motivated to join this particular startup as the CPO because I see an opportunity to really move the needle on defense. And in particular, to help these hard working folks on cyber defense teams that we just talked about who have these, you know, relentless, stressful, overwhelming jobs. Basically, I want to help the humans of cyber. There are some key startups working on new technologies that I think are gonna find the shift the balance of power, more in favor of defenders. And, you know, I'm thrilled to be part of that. So keep an eye on this space. And maybe when we come out of stealth, I can come back and we can discuss my my particular startup a little bit more.

K Keith Hawkey 31:00

Ah, so vague, so vague, not enough information. But we'll, you know, I definitely when, when, when things become clearer, and the incubation is now open to the market I'd love to have you back on. But I'll tell you that the most important question I have about stealth is, and this this is the question I get most I mean, so you're probably going to have like a light mode and dark mode to the platform. But what my seven year old son wants to know is when are you coming out with a rainbow mode. When when is rainbow coming?

W William MacMillan 31:38

Well, I obviously can't give away any trade secrets, you know, we're working on our intellectual property now. But I will, you know, as the product guy, my responsibility is to the backlog of features and functionality that we're going to build into the platform. I will take this back to the team, and I'll make sure that we're prioritizing rainbow mode.

K Keith Hawkey 32:00

There is a marketplace, I'll tell you. So,

W William MacMillan 32:03

You're out there in the market, I believe you.

K Keith Hawkey 32:07

Yeah, dark mode, light mode, rainbow mode. Now, here we go. It is it is funny how, I'm on tech demos all the time. And the sell for for dark mode is I mean, most platforms have a dark mode today, and but but you know, the reps that are on these tech demo calls are all very excited to announce that they have dark mode. And it's like, oh check it out, Dark Mode. William, I really appreciate the time that you've spent today, with us on the IT Matters podcast, I want to make sure to include all the documentation and you know, the people that you pointed out and the organizations that are supporting CIA in cinema. I think that's a valuable enterprise and it only leads to a younger generation that is poised and prepared to take on a life of service, which is much needed in our civil services, in our in our military service, and government service is is eager and dedicated young people that are that are willing to make the sacrifice for for all of us. So I want to make sure to include that. One of the important elements of the IT Matters podcast is a sense of community, a sense of being able to bounce ideas off each other. We have a lot of IT leaders that tune in, where can people find you, William, if they have a question about one of the topics we discussed or they'd like to pick your brain on something, if interested in stealth when when Stealth is is released? Where can people find you him?

William MacMillan 33:47

Yeah, great question. So old habits die hard. And as you might be able to imagine, retired CIA officers aren't usually hugely into social media and a big web presence. I do LinkedIn. And that's really the primary space that I'm active in. When we come out of stealth, our company will also have a website, you'll have the ability to reach out to us that way. For now, it's probably LinkedIn, just following events that I'm going to attend and that sort of thing. But we'll be a little bit splashier, once we kind of announce what we're working on and get out there into the marketplace.

Keith Hawkey 34:23

So you're telling me that former CIA leaders aren't major influencers on Tik Tok?

William MacMillan 34:29

Yeah, we're not on Tik Tok. I don't I don't want to get into any proprietary debates here. But you know, I don't have Tik Tok on my personal phone, let me put it that way.

Keith Hawkey 34:40

Yeah, you and I are the same. Well, I'll make sure to include your LinkedIn information in the call notes. And is there any last word and you know, I actually I'd like to ask you a question about the younger generation right before we leave. If we have, we have some of the IT visionaries that listen to the podcast, but we also have a younger audience that want to get into the industry want to make an impact and are eager and excited, and particularly when it comes to defending our nation in the IT and cybersecurity space. What kind of message would you would you tell a young person that is interested in this career? And do you have any guidance that you might impart?

William MacMillan 35:21

Yeah, I would say there's several things, right. So people reach out to me and asked me about this all the time. First and foremost, I can't emphasize enough, I don't know why people wouldn't want to work in cybersecurity, like it is where the action is. It's super fun. It's an incredibly dynamic field. It's transforming a lot right now after, you know, after a period that a lot of folks would argue the technologies were sort of stagnating. And you know, we were we were kind of mired in the same problems, there's a ton of optimism, it's a very dynamic place where you just can't get enough cyber talent nowadays. So it's a wonderful place to try to set yourself up if you're a young professional looking for, you know, what vector should I head out on for the next phase of my career. In terms of how to approach it, just jump in and start is my overwhelming guidance to people. Like I, folks will reach out and they'll be a little wrapped around the axle about, you know, what certification do I need? What, what training do I need? How technical do I need to be, I'll use myself as an example. You know, I've worked in cyber for a long time now. And I'm not deeply, deeply technical. I don't have you know, a computer science engineering degree or anything, I have certainly had to take training and go back to school and do all of those things. But you can do that along the way as you're immersing yourself in it and learning the field. So the main thing is get out there. Interact with people, cybersecurity people like to pretend that they're very surly, and curmudgeonly, especially at the sort of, you know, more senior executive level, because it is a stressful field. But the reality is, if you reach out to folks, and you seek mentorship and advice and guidance, I think most people in the field, they want the help, they need the fresh talent coming in and they're generally really willing to connect on a human level and sort of describe what it's like and give folks guidance. So you know, get out there, get in the mix, take that first job, take the leap. You'll love it. You'll be able to learn as you go and figure out you know which of the many, many corners of cybersecurity you want to kind of head into first. There's a lot to do out there and we're waiting for you. So come on.

K

Keith Hawkey 37:25

So come on, he says. I think that's an excellent note to leave on. Feel free to reach out to William and thank you for tuning in to the IT Matters podcast. We'll catch you next time.

W

William MacMillan 37:37

Thanks.

N

Narrator 37:40

Thanks for listening. The IT Matters podcast is produced by Opkalla, an IT advisory firm that helps businesses navigate the vast and complex IT marketplace. Learn more about Opkalla at opkalla.com.