Detroit Mercy Cybersecurity 313 Podcast no.13 - Richard Richard H.L. Marshall

2/8/2021 45:59

Richard H.L. Marshall has over 20 years of broad executive leadership experience in cybersecurity and national defense. He has served in the U.S. Department of Defense, National Security Agency (as the legal architect of nation's first cyber warfare exercise), the White House, the Department of Commerce and the Department of Homeland Security as director of Global Cyber Security Management. Join us as we listen to this interesting discussion with the man for whom we named the Center's Cybersecurity student of the year award.

A **Announcer** 00:01
This is the Detroit Mercy, Cybersecurity 313 podcast.

T **Tamara Shoemaker** 00:07
Hello, this is Tamara Shoemaker, the director for the Center for Cybersecurity and intelligence Studies at the University of Detroit Mercy. My guest today is Dr. Richard H.L. Marshall. Richard, it's a pleasure to have you here and to see you. It's been quite a while since we've actually been in person together, we spend a lot of time in the DC area together with you, as you were helping our center, you were a Vietnam vet pilot, you got your JD and Georgetown, and you were at the Citadel. And we've had all kinds of wonderful things. You're an SES officer, or the federal government for years, and many, many different places, if you could expand on a bunch of all that kind of stuff so that people can get an idea of who they're talking to.

R **Richard H.L. Marshall** 00:46
Well, I think my friend Tambora has already told you that I've had a checkered past. Some good, some bad, but all of it has led to where I am today. You know, as a contributor, I will

do as the young kids would say, a shout out to the senator, which is where I went to college. That particular environment, really shaped my whole life going forward. Now, there were a number of other life changing events. And I won't go through all of those. But I think it's very, very important, where you get your initial educational training, and who you are working with, and try to get good mentors that will help shape your life philosophy and keep you focused on success. That makes a tremendous difference on where you're going. And a secondary point would be, never give up when you think you've hit a wall. Some of my colleagues will say, My God, rich, you're great at reinventing yourself. Well, I think that's part of my upbringing, both from my parents, my religious background, and my scholastic background... Is that don't look in life's rearview mirror, that's not where you're going, look in the windshield, and see where you're going and help shape that destiny and take advantage of opportunities that come along. There have been mentors in my life that I didn't expect. And I was lucky enough, I would like to say smart enough, but in reality lucky enough to listen to them. So enough of that Balderdash. Let me give you some basic points. I'm a recovering [type] A personality, which you probably picked up on. I'm also a recovering attorney. Although most of my work lately has been associated with international law. And I spend a lot of time doing international law. I'd rather do cybersecurity policy. Because to me, that's exciting. I know to a lot of people, that's boring. But I cut my teeth on that, so to speak, at a late age. Now, many, many years ago, when I was the associate General Counsel of information system security at the National Security Agency. And let me translate that. NSA has two basic missions, although they don't like to phrase it that way. But two fundamental areas of practice, shall we say. One is to intercept the adversaries communications—intelligence data—to use the role term, to help our key policymakers make appropriate decisions. And, more importantly, to protect the American way of life related mission is associated with making sure that our communications are adequately protected, so that the adversary can do the same thing to us that we're doing to them. Now, correctly, those two activities are combined at the National Security Agency. And here's why I think that's a good thing. If you're very good at breaking signals, then it would correspond that you can take some of that language or some of that knowledge about how to break signals into how to protect them. And if you're very good at protecting signals, then that makes it easier for you to figure out how the adversary is protecting their signals, so that you can break those. Now I know that sounds a little more exotic than it actually is. But let me translate that into a more application layer level. We were very interested in protecting DOD [Department of Defense] and Government Communications from being intercepted by the adversary. And initially, that was radio communications for all intents and purposes, and telephonic communications. But in the late 80s, early 90s, it became more and more associated with computers. So that was a big paradigm shift to where you're not intercepting RF frequencies. You're not intercepting telephone calls. You're not intercepting various communication networks. What you're doing is entering into the cyber arena, and trying

to figure out how to protect our systems, and how to exploit the adversary systems. And that became a very fascinating challenge for all of the missions associated with NSA. Now, as I mentioned, I was the Associate General Counsel for Information System Security. And one of the activities we were involved in on that side of NSA was attacking. with permission, the government telecommunication systems, read into that computers to make sure they were secure. Now, as a lawyer, I was very concerned about making sure that what my team was doing was legal. You know, I wanted there to be a situation that if my clients were in jail, I would go there to visit them, not being an inmate with him. So in order to understand exactly what they were doing, I asked to be trained to do what they were doing. So you're looking at a hacker. Now, I'm no good at it. I wasn't that good at it at the time. But I understood their thinking, and some of the applications and why it was so important to understand that in order to give a legal judgment, not a negative, I mean, a lot of lawyers learned in kindergarten to say no and never migrated from that. But the good lawyer helps the client, understand how they can achieve their objectives. So the Telemark for that was an exercise called eligible receiver 97. It's in the history books. Now, I've been interviewed quite a few times, both on television and the subject of a couple of interesting epilogues in books. But basically, we were given the opportunity to attack a major warfighting sink commander in the Pacific. And we did that under a very unique way. One, because you don't want to violate 18 USC, that's a criminal statute doesn't do much for career progression, because then you run the risk of going to jail for a year or more. And the other activity was associated with... there was an executive order that said NSA had the authority to do this, number one. But being the cautious attorney that I was, I was looking at 18 USC, which gave me an exemption, if the owner of that telecommunication systems gives you the permission to test it for efficacy. In other words, making sure it's safe to use, then you've got a green light to go ahead. So the challenge was, we had to determine who was in charge of the DOD telecommunication system. And oddly enough, we reached the conclusion that it was the secretary of defense. So we had to get the secretary of Defense's permission, but in order to get his permission, he said, talk to my lawyer. So I had to go and talk to the DOJ General Counsel at the time. And I invited the NSA general counsel to go with me and he says, No, Marshall, you go by yourself, you know what you're doing? I have full confidence in you. Well, that was a nice thing to say. And I really appreciated that. But I didn't realize the full implications of what that meant. until after I had briefed the DOJ General Counsel. And she was satisfied with what we were doing, and said, I think what you're doing is legal. But I really would prefer if the Attorney General said what you were doing was legal. So I go and talk with her. And I said, Yes, ma'am. I'm happy to do that. I'll set up a meeting and both of us can go. And she said no, I have full faith and confidence in you. You go by yourself.

T Tamara Shoemaker 08:49

Richard, am I sensing a deniability issue going on here with you?

R Richard H.L. Marshall 08:54

Well, you're very perceptive, a lot more perceptive than I was at the time. And basically what it was they wanted to have plausible deniability and be able to say, if it didn't work, we always knew that Rich was crazy anyway, and let it go with that. So I briefed Janet Reno, who was over six feet tall, very formidable person. And what most people don't realize is that she worked her way through college and law school wrestling alligators. Now, the fact that she was still alive suggested that she won all of her wrestling matches with alligators. So she was not only formidable from a physical standpoint, not that she threatened a physical harm. But she was an intellectual giant. It was amazing to have the wonderful conversation that I had with her, and we became fast friends as a result of that. So there again, is an example of you never know who's going to be on your side until they happen to join forces with you. So I'm happy to say that she served as a mentor to me and helping to develop what is my career. Now the acting president in this exercise was a fella by the name of Richard Clarke. Most people refer to him as Dick Clark. And I'm sure many of you are aware of the fact that he became the cyber czar are under the president at that time, which was Bill Clinton, most people didn't realize that initially, and then later under bush as well. But Mr. Clark, or Richard Clark, became a cybersecurity expert self appointed, as a result of his experience as being the acting president during eligible receiver 97. And I had the great opportunity to work with him, actually, for him in the White House, helping to develop cybersecurity policy. So this was a great opportunity to take advantage of what I knew, technically, which was a mile wide and an inch deep. But I had a lot of friends who were very good in the technical field, and could call on them. And that helped formulate some national strategy. And as a praise to Richard Clark, at the time, had the policies we developed and promulgated during that tenure, had they been approved and implemented, we would not be having half of the problems that we're now having with cybersecurity, technical issues. But once again, it was a situation where things were over coordinated, and vanilla ized. Because even today, we still don't have an entity that's in charge of cybersecurity for the United States. It's very diffused. And it's very diffused, because everybody wants an opportunity to get a little bit of money from Congress. So everybody lays claim to be unable to do it, but very few can deliver. And I think we've seen that with a couple of recent exploits, by our adversaries. And I won't get started on that, because it is just too frustrating to talk about. So my main focus area is in policy. And as a result of that, and looking around and knowing that we needed to have adequate technical talent in the federal government, I had the opportunity to be involved in helping to establish a cybersecurity program for colleges and universities throughout the United States. Dick Clark was a major proponent of that. There was also an individual from Idaho, a deep personal friend of mine, who played a key role in that, and the

Director of Information Systems Security at NSA was heavily involved. And it was just a great group to work with, to put together this particular program, which has grown over the years and is very active. And one of the big pluses of that was not just to helping to develop the policy, but to implement the program, and to be part of that program implementation. And that's where I first met our hostess with the mostess. camera and her charming husband. And we looked around, and each of the schools gave a presentation on why they should be part of the program. And I'll be quite honest with you, and I've said this to Dan and Tamara before University of Detroit Mercy. Who are they? Aren't they a bit presumptuous to think they can be part of this great program? Well, they certainly taught me a lot. I listened to their presentation. And I said, you know, they have it together. I want to be part of them. Because everybody wants to be on the winning team. You know, Coach pick me. So I got to be friendly with Tamara and Dan. And I realized what a great program they had. And so when I came back to the fort, I said, I want to be there seal, which is an acronym for senior executive, academic liaison. Now, at that time, I was Senior Executive Service, the equivalent at that time of a one star generals. So I had a little bit of leeway on an opportunity to express my desires and get away with it. So I was very happy to be selected to be their seal. And it was just an overwhelmingly positive experience on both sides, not just for me, but for Tamara and Dan and for the University of Detroit Mercy. So let me beat the drum a little bit for UDM [University of Detroit Mercy] One of my very dear friends, John Waters, who headed up a major cybersecurity company was very impressed with the program. I took him up there with me to meet the head of UDM and discuss their particular program. Now, John had a vested interest because he was always looking for talent in his cybersecurity program. I was interested because A, I thought John could get some good resources from UDM, although he was going to be competing with NSA, but you know, whenever there's competition that brings out the best of people with John was so impressed with what was going on at UDM that he pulled out his checkbook and wrote out a check. I think it was for 10 or $20,000. I don't remember exactly, but it surprised me quite a bit, and then handed it to the head of UDM. I mean, that was his commitment right away. Now, let me tell you another good thing about UDM. And I'm still involved with UDM. But, and I think this is still true. It's been about two years since I've checked the statistics. But the University of Detroit Mercy has more cybersecurity trainees graduates in the National Security Agency infosec program, per capita than any other college or university in the United States. So that says a lot about UDM. Now, I should be fair to the other schools that I was involved with, as their CEO. I was also the CEO for schools in Boston. One of them was Boston University, produced a lot of good students. Most of them are in the private sector, also formulated a program there that combined cybersecurity with their MBA program. And this was 12 years ago, it was unheard of to do that, at that time. The other school that I was associated with, was Northeastern University. Two points to remember there. One, my daughter is a graduate of Northeastern, so I'm going to beat my chest about that a little bit. So I'm very proud of her

successes. But more importantly, Northeastern University had more US citizens, most of them female in their graduate cybersecurity program, than any other institution in the United States. Now, I asked out of curiosity, intellectual curiosity. Why? Why Northeastern? The answer was, there's a lot of smart people that come to Boston to go to college, I think somebody said, was it half the people who live in Boston are graduate students, or college students, I don't know, a lot of them. And they said, smart people tend to hang out with smart people. So you have one half of the couple in one program, and the other half of the couple are in another program. And we just have been able to take advantage of a lot of people who want to be in the cybersecurity program. In point of fact, Northeastern graduated, the very first US citizen, PhD in cybersecurity. Big, big. This gives me an opportunity to beat the real drum that I want to be. And that is STEM education, science, technology, engineering, and math. Not to be disparaging of college students who can't get jobs. But I think the reason they can't get a job is because they did not major in a competitive degree. I'm not against soft subject degrees, they play a role. But if you have a choice, to get a degree in cybersecurity, you have a job waiting for you at the end of that, you don't have to worry about paying your student debt, you've got two options. You can work for the federal government for a period of four years, and then take care of your student debt. The other thing you can do is work for the private sector, and probably pay off your student debt in one to two years. Because the private sector pays so much there is a continuing and growing need for cybersecurity professionals. Now, that doesn't mean you have to necessarily be a programmer. It doesn't necessarily mean you have to be a very technical analysts. What you do have to be conversant and have a good background on science, technology, engineering and math. And that can be combined with a business program. It can be combined with philosophy. It can be combined with other liberal subjects, to have that grounding in STEM education, helps you get a job, and not just a job where you're making 12 to $15 an hour. It's a job where you make a living wage, you can buy a house, you can make a car payment, you can raise a family. So I'm very big on that particular arena. Very big on cybersecurity education. But again, you don't have to have a PhD in cybersecurity, to be successful, just understanding what it is in the business world, up until recently, and I think this is still the case, with a lot of boards, I am an advisor to either five or six boards. And I emphasize them that cybersecurity is a leadership issue. And they always give me pushback and they say, no, it's a propellerhead issue. It goes to the cyber geeks. And of course, they don't like to talk to the cyber geeks, in part because they don't understand them. And also because they fear them. Because most people who are CEOs are pretty smart. And they just don't, they're not able to communicate that effectively with members of the board, not as a result of the CEOs failure to articulate what's going on. But the result of senior board members who just don't understand it, and don't want to understand it. But once I am able to educate them, and help them understand that it's a leadership issue, it's a due diligence issue. It's an issue that they need to be involved in, because everything you do in business, is on a computer now. And

if you don't protect your ability to do business, you lose, you lose business, you lose clients, you lose money in the stock market. And there is an increasing possibility of liability may not be direct liability. But if you're a board member, and you've had an attack, and you were not able to protect against it, the stock price drops. And when that happens, the shareholders want to get rid of the board members that they think are responsible. And it's very difficult to raise a defense was all I did the best I could, that doesn't work. It's a zero sum game.

T Tamara Shoemaker 21:55

We're going through some of that right this minute, right? We have some major major players, agencies that have been hit, and the C level suite is getting a big hit. The techies aren't taking a hit. And it was definitely a combination effort of things that didn't work out. Right. And again, I think the thing that's cool about you is that you have this policy background. And if we went back to the like you said, if we went back to some sound policies that had not been followed, if they had been followed, we wouldn't be having those discussions all over the country right now. And many, many people wouldn't be losing their jobs because of things that didn't happen the way they should have.

R Richard H.L. Marshall 22:29

Well, there's a lot of finger pointing exercise, it wasn't me it was him, just the fact that I got hit. I did everything that I realistically could do. But the software that I bought, or the software system that I licensed, or the updating system that I paid a lot of money for, it didn't work, it's not my fault, it's their fault. Well, I'm going to invoke the North Dakota doctrine or bullous, rauris, it is your fault. Due Diligence would require you to make sure that the food chain, the chain of custody, how everything works together, works together. And you need to go back to the very beginning, and chase that chain of custody, to make sure everything is legitimate. And as I tell the members of boards, you do the same thing when somebody invests in you, you track the money, you do the same thing, when you are investing in a company, you do a significant amount of due diligence to make sure that they are legitimate, that they are sound. And that's going to be a worthwhile investment. Why don't you devote that same amount of energy and intellect and money to make sure your cybersecurity program to make sure your business program is safe from cyber security attacks. Don't blame somebody else. Don't hold anybody else accountable. You're the one that needs to be responsible and needs to act that way. So when you have a company like fireeye, and I have personal friends who run that company, I need to do that disclosure. But what they did took a tremendous amount of business leadership. They could have swept it under the rug like others have done. They could have ignored it and hoped that it would go away like others had done and I won't mention names. Yeah. But

they took responsibility. And they said, there is what happened. Here's what needs to be done to help correct it. Now I realize it was after the fact. But correct ended after the fact is much better than ignoring it. And then we should give due credit to Microsoft who said, okay, we need to take action to help correct this problem. So what we're going to do and it was a policy decision that was technically implemented, is we're going to check to make sure the certificates are timely and accurate and still worthwhile, and they nullified a bunch of certificates that were not acceptable anymore and replace them with new ones. So that took out a channel of access for the adversaries. Now, that's wonderful in hindsight, and I'm not trying to beat up anybody here are pointing fingers. But it illustrates what we should be doing all along. Every single moment, we should trust, but verify it. I'm not saying that as a political statement. I'm saying that as a business statement. When you get in your car, if you're smart, you need to check to make sure you've got enough gas to get wherever you think you're going. You put on your seatbelt. You look at traffic before you move out in it. You decide where you're going to go and how much time it's going to take you to get there, etc. My point is, you plan ahead. Right. And a lot of the plan ahead has been lessons learned from prior mistakes. Why don't we do the same thing with cybersecurity. So again, you don't need to have a PhD in cybersecurity to help make a difference. You just need to be aware, and to help implement some positive change.

T Tamara Shoemaker 26:15

I think this really illustrates how business and techies and all this stuff has to work all together. It's a concert, right, and you have all the different pieces and parts that work. But they have to work together, right. And so I think the cool thing about cyber and you've done it even in your own career, you talked about earlier was that there are different pieces and parts that you've gone from one to another. So there's no one thing that you can study, one thing that you are going to be one thing that is going to do it all, there's no silver bullet, right, there's no magic, whatever. But it's how it all works together. And then how your career moves through as well. In cyber, there's a ton of different things. So you're an attorney, and you have an amazing career in this area. And you weren't trained in technical stuff, although you've brought in some of that stuff later in life. And you added that to your quiver of tools that you could use, right? Our students are the same way in our adult learners and people who are just trying to keep themselves safe, right? These are all things that we need to start learning and start incorporating into our thing, but never stopping, right, we always are moving forward, always learning new things. So hopefully, we're going to take from this emergency, a whole lot of learned lessons, and then go forward with a little bit more knowledge and working together more on some of these things.

R Richard H.L. Marshall 27:28

Oh, definitely one of my most enjoyable experiences was my two years at the Department of Homeland Security. Although there were times when it was very, very frustrating. I was the senior non political appointee. So I was very frustrated that some of my senior leadership was reluctant to make a decision. And there were some interesting workarounds, which I won't publicly disclose. But the point is, I was the director of cybersecurity management for the Department of Defense, which was basically for the United States government. And I enjoyed my job so much, because I was working with 25 to 30 individuals who had degrees in cybersecurity. I was a lawyer. But I was in their view, an effective manager, because I help them focus on the areas that we need to focus and become very productive. But even though they were young enough to be my children, literally, I learned a tremendous amount from them. Not just technology, but new management skills, things like remote working, which was unheard of at the time. Now, that's all we do, which is created another avenue of opportunity for the adversaries. That's another opportunity to be heads up all the other activities in my life, it made a big difference was attending and actually participating as a speaker at RSA conference in California, which they don't have in person anymore. But more importantly, black hat and DEF CON in Las Vegas, which sounds like a hell of a lot of fun. And it was because you got to meet with a lot of fascinating people. And I remember two points I want to share with you here. One, I took my son with me whenever I went to Las Vegas. Now a lot of people would say that's crazy when my son was over 21. But when I took him out there, I had him involved in what we were doing. I had him volunteer as a goon, which is a polite way of saying he was a helper. And his job was to escort speakers to various locations to make sure they got where they needed to be on time. Now, the positive of that was he got to meet a lot of fascinating people, which kind of helped shape him. And now through no fault of my own. No pressure. He's an IT guru. And yeah, you know, so the point is You can't teach them young enough, give them an opportunity expose them, even if it's in a non technical way, and watch to see what happens, watch to see how they blossom. Watch to see how they grow. just fascinating, absolutely fascinating. The other aspect of working with these young kids was I learned an awful lot from them, not just technology, but how to better manage a large group of people, whether they are in house, or whether they're out house, you know, right now, because of COVID. Most people are working from home now, and thriving, and doing well. It's a plus and a minus, you know, you save a lot of time, and you're not having to commute. But the other disadvantages, so many systems at home, are not adequately protected, we're getting better at it. But everyone in the home environment needs to be more conscious of cybersecurity, it doesn't mean they need to be an expert. But it just means they need to do some very basic things. If you're a Microsoft user, every second Tuesday of the month, you need to upgrade your computer, you need to put in patches, it's called Patch Tuesday for a reason. Patch Tuesday is followed by hacker Wednesday, because the hackers get the same information. And you

get and they exploit those vulnerabilities that you have chosen not to install, or ignored. And sometimes it's ignored from a business standpoint, for very complex reasons, particularly in the financial sector, they have very specialized software. And before they install a patch, they want to make sure that the patch doesn't have any adverse impact on the software. So they can't install overnight, like the home user can presumably, and the adversary takes advantage of that. So it's a requirement of being constantly vigilant.

T Tamara Shoemaker 31:59

I talk about it because I work a lot in the K through 12 space now trying to get that pipeline full of folks that are really excited about these career of fields. I talk a lot about being like hygiene, right? Yeah, you know, it's just really good hygiene with your computer and whatever. And so if you think about it, not quite so I don't know, high tech and scary and that kind of thing. But just really good basic principles that you use to make sure you and yours are safe. You know, everybody is going to be more enriched and more protected. If we all take on that responsibility, right? In try to make sure that we do the best we can with our systems and everything that we touch.

R Richard H.L. Marshall 32:34

Exactly. Let me add another comment about UDM. And I don't mean to embarrass your camera, if you blush, that's okay. But you and Dan have just been absolutely fascinating and fantastic in terms of bird dogging some of your top students to me, and who are going to be in the Washington area either as visiting, or maybe working in the area. And you give me an opportunity to serve as a mentor for many of these. And that has been a tremendously rewarding experience for me, both from an ego boost, because you picked me. And also it shows the results of what you and Dan have been able to do up in UDM. So I get to see your quality products that are directly attributable to the education and training that they get to UDM. And I need to brag on the most recent one you sent me. And I won't mention her name. But when she interviewed for NSA, and this is unheard of when she interviewed for NSA, she was offered the job at the end of that interview. That never happens.

T Tamara Shoemaker 33:39

No, that's cool.

R Richard H.L. Marshall 33:40

That's my knowledge that has never happened.

T Tamara Shoemaker 33:43

Yeah, we're pretty pleased with that. And I got to give that right back to you, though, Richard, because I know that you spent an awful lot of time with that student mentoring her as you have many of other folks that we brought up. And just like many of the mentors that I use now with the K through 12 stuff, once again, you thank me for the opportunity to mentor our students, which it's an honor for us to have you as a mentor, and for them to have you a mentor. I mean, I can't even imagine where I might be, if I had started out young in life, being able to have a mentor that was x senior executive and is one global executive still mentoring my career. So I mean, these kids have gotten some amazing opportunities because of our affiliation with you and with the NSA and the things that we've done with the center that we just couldn't have done without your help. And thankfully, I hope that you are honored by the fact that each year we have a grad student that's voted the cybersecurity Student Of The Year and that award is called the Richard H. L. Marshall award. And we do that in service to you. And we want to make sure that your legacy is remembered here and all the things that you have given us all the opportunities, all the doors, you opened all of the things that we learned from you, but our many trips to DC back and forth. We've been very, very fortunate. We were very lucky that back in 2004, 17 years ago. Can you imagine that that how long it's been we met and We were able to take the fledgling of our center and just start to grow it with your help and your support. And over the years now, all the graduates that we've had, it's amazing, we're ranked one of the top three and online degrees that can be done in a year, all the things that we've been able to do, we just couldn't have done it without the people that have supported us over the years, and you are one of them. So I've been very excited about being able to talk to you on our podcast about this and sort of how things all went. As we get close to the end, I would love for you to tell us a little bit about some of the stuff that you're currently working on. And you would like to brag on. Now, as always, with Richard everything has to be carefully monitored not to let out too many things as far as secrets and things like that, which is also kind of cool. Just to know somebody that has secrets. Can you tell us a little bit about some of the stuff that you're currently working on?

R Richard H.L. Marshall 35:48

Yes. And let me make sure I'm appropriately reflective on this. Two things that I want to talk about. One is T.E.A.S. I'll break out that acronym in a moment. And the other is what we are going to be doing in a Middle Eastern country associated with a data center. Now, you may say what in the world does that have to do with what we're talking about today? And I'll explain that. A few years ago, I got approached by an entity called Aqua Comms Aqua for water comms communication, who had just put in a new fiber optic cable system from New York to Ireland. And at the time, it had the lowest latency meaning the fastest speed and the largest capacity of any underwater cable system in the world. And they

approached me to help them extensively to get government contracts. And I need to stop at that point about Aqua Comms. But that relationship that was developed with the CEO of that company, made a difference in my life later, which I didn't realize was going to happen at the time. But as all too often happens in major companies, a new investor comes in and wants to replace the CEO with their own hired gun. And so the colleague that I had worked with for some time, at subcom, even though he lived in Ireland, he was a US citizen, he was issued a parachute. It wasn't completely golden, but it was attractive enough. And he went back to Houston, where he had a home and got settled there, called me and said, Rich, let's form a company. And I said, Well, what are we gonna do? And he said, Well, I think we need to form a company that's gonna put in fiber optic cable systems in the world. And I said, You've got to be crazy. I'm not experienced at that. I don't have what needs to be done. I think you've got a great idea. I think you're highly capable. But I'm not your guy. And they said, No, I think you are. And he explained some reasons that were convincing to me. So I said yes. And so we formed a corporation, incorporated in Delaware. And we named it Cinturion Corp with an eye, which is the same as the Roman Cinturions, but we use the Spanish spelling, because we could get that registered as the name of the company. So we formed a corporation in Delaware, Cinturion Corp, and we were off to the races. And I got a phone call from him saying, you know, I've been approached by some clients that I can name at the moment, who would really like to have a new route going through the middle east to India? I said, What's wrong with the current route? Well, it's antiquated, his service disruptive. It goes through a country that takes advantage of people economically. And they want to have a new route. So he said, Well, the preferred route of our clients is going through Israel. And I said, Greg, I realize you're very technically competent, but I'm sure you know enough about geography, to realize that Israel is in the middle of the Middle East. And it is not the most attractive area to do business. And he said, Well, if anybody can help make that happen, it's you. And I said, Okay, Greg, I appreciate your blowing smoke, but I recognize it. Let's change the subject, but he persisted. And then I started thinking, I said, No, wait a minute. I think I know somebody who knows somebody that can help us. And I played those cards, and was able to locate a good business partner in Israel who was extremely helpful. So what that has led to is that as of tomorrow, we will be fully funded to proceed with our project, which is to put in place, a new fiber optic cable system, the fastest speed, the largest capacity of anywhere in the world, from France, Italy and Greece, under the Mediterranean, landing in Israel going across Israel, on land, terrestrial, going into Jordan, going around the top of Saudi Arabia into the Red Sea, going down and around Saudi Arabia, going in to India, which is where we want to go, and then later going to Singapore, Malaysia, and then possibly in the out years to Australia, New Zealand, and maybe even Chile. So it'll go around the world. Massive, massive program. Absolutely amazing. Now, what we've been able to do in the last couple of years, completely unforeseen is Israel, Jordan, and we're also doing business in Saudi Arabia. Now, when I was in Saudi Arabia,

and explained to them what we were doing, at that time, that they did not even want to admit Israel's existence. Now, things have changed in the last four years, in the last two years, particularly even in the last few months, if you really want to put a fine point on it. But I explained to the Saudis that we were connected to Jordan, and they were happy with that. So over time, the Saudis and the Israelis are doing things diplomatically, that they weren't doing before. Now, I'm not saying it was a result of Cinturions activities in the Middle East. But we did give them an opportunity to have yet another opportunity to communicate and communicate effectively. And so we have investors, both from Israel, and Saudi Arabia, in the cinterion, which is a US company. Now, to me, I'm not saying that's gonna lead to a peace prize, but it's just absolutely phenomenal to think that that was an unanticipated result of these activities. And now, some of my friends are saying, Oh, my gosh, aren't you worried about the potential for changing political dynamics in the Middle East, in terms of..

T Tamara Shoemaker 42:41
Right, they've always worried about whenever there's any political changes, that things are gonna happen differently.

R Richard H.L. Marshall 42:47
Exactly. But we can kind of take comfort in the fact that people need to communicate, whether they're fighting with each other, whether there's times of military or, or tension, they need to communicate. And this new fiber optic cable system gives people the ability to communicate more effectively. Now, let me add one other thing. There's a particular Middle Eastern country, which I am not permitted to name at the moment that has never had a data center. Never. We are in negotiation with a country to install a data center. And that data center is going to be staffed primarily with females. So this is another landmark achievement in the cybersecurity arena. So I mentioned that story, because I don't want women around the world. To think that cybersecurity is a guy thing. It is not, it is an equal opportunity for those who want it. So I encourage everyone, regardless of what sexual identity they may claim, to focus on science, technology, engineering, and math, education. Even if you're skimming the surface, get comfortable in that particular arena, because it will pay tremendous dividends to you personally, and will also help not just the nation's security, but the world security.

T Tamara Shoemaker 44:19
I totally agree.

R Richard H.L. Marshall 44:20
I'm off my...

T Tamara Shoemaker 44:21
...Soapbox. No, we love it. I love all the stories. My listeners will enjoy all this. Some of the backgrounds, some of the interesting things that you had to say about all these things, we truly value the fact that you made time for us and you didn't have to come to snowy Michigan in order to do it. So

R Richard H.L. Marshall 44:37
Oh, yes. Well, I've been to snowy Michigan, and I've gotten stuck here.

T Tamara Shoemaker 44:43
And snowing Michigan on a timer, as well, and that kind of thing. But we didn't have to do any of that. But we got to visit and so it's been a pleasure. And I truly thank you for joining us on this podcast today.

R Richard H.L. Marshall 44:53
Let me conclude with one other comment. I started early by saying how important it was my colleagues experience at the center of all the other school that has paid a tremendous influence on my life is UDM. Working with you guys has just been absolutely life changing, and absolutely phenomenal. You've made a significant positive impact on my life. And for that I'm eternally grateful.

T Tamara Shoemaker 45:19
We feel exactly the same way. It's definitely all of us together again, and I truly appreciate your time. And we look forward to talking to you again real soon.

R Richard H.L. Marshall 45:29
Excellent, very good. Thank you for the opportunity.

T Tamara Shoemaker 45:32

Thank you.

A **Announcer** 45:33

You've been listening to the Detroit Mercy cybersecurity 313 podcast. If you would like more information on today's discussion, please contact center director Tamara Shoemaker and by emailing sh o EMTL at Ud Mercy.edu. And please plan to join us again for the next edition of the Detroit Mercy cybersecurity 313 podcast.