# Detroit Mercy Cybersecurity 313 Podcast no.15 - Dave Trader

Thu, 3/11 10:43AM 41:36

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

T **Tamara Shoemaker** 00:07
Welcome to the 313 Podcast at the Center for Cyber Security and Intelligence Studies at the University of Detroit Mercy. Today, I am talking with a good friend and a member of our advisory board here at the University of Detroit mercy, Dave trader, he's the CISO for Presidio, and I met him and his lovely wife, Jenny many years ago, and we have been friends. And we've watched his career go up, up, up, and I can't wait for him to tell you a little bit about himself, and the pathway that he's taken in the cybersecurity career.

D **Dave Trader** 00:41
Excellent. Thank you so much for having me. I really appreciate it. I started my career in the United States Marine Corps, back in 1998. Seems like forever ago now. In my focus back then was was based on encryption. And we used to take encryption and wrap it around communications. And didn't matter where that communications went, it could be satellite communications, radio communications, ship to shore. And then about that time, we started getting into siprnet and differnet. Moving through on the network side. So I got

to kind of kick things off on the intelligence side, and was attached to first battalion 24th Marines, and ended up finishing out my career there. And after that, I didn't know what I wanted to do for a little while thought I wanted to go into law enforcement on the police officer side, and just started seeing that I liked doing police work, I was a police officer for northville Township for a little while and really liked that. But it just wasn't enough for me, I wanted more. So I started going after every certification in cyber security that you can imagine. And I think I have over 70 today from just leveraging some of the different avenues that the federal government kind of provided for veterans to get into that space. So I just took full advantage of that, and just one right after the other just kept going. And then I became a CISO at Galaxy Solutions, and was there for seven years and as a software development company and had responsibility internationally with them and got quite a bit of experience as a CISO in learning all things on the infrastructure in the cyber side and building out the sock and then also protecting the products that we had, you know, we're shipping software. So knowing what the SDLC look like, and what the gate checks look like and how to do dev sec Ops, a lot of fun experience out of that, and then moved into a consulting role in 2019 as a cybersecurity practice lead for Presidio. And that brings me up to where I'm at today.

T **Tamara Shoemaker** 02:28

Very cool. Can you tell us a little bit about Presidio? So the folks know what kind of company this is that you work for?

D **Dave Trader** 02:33

Sure, absolutely. So Presidio has been around for a long time. And they primarily focus on digital transformation. And they're historically known for kind of full stack services and routers, and switching and network architecture and data center and collabspace. And everything you need to build out an infrastructure in what you've got at the enterprise level, and cybersecurity, they've added that in the last 5-10 years. And they've also invested heavily in that through acquisition of some great companies that have come on board. And today, the cybersecurity practice alone is a $750 million business. So they're massive on the infrastructure side, a lot of heavy advisory services, professional services, we do everything from staff augmentation to smart hands in the field, just as numerous things we can do. But the one thing I liked about Presidio was, when I looked at where I could go for consulting, I didn't want to give my customer homework, I didn't want to have to say, Well, this is a switch problem. Or you've got this vulnerability that exists in your collab software in a communication. So you have to go do this mister and miss customer, you have to go do this, and then come back to me. And then I can reevaluate. I didn't like that style of consulting, I wanted to have the ability to say, you don't have to do that you

can if you'd like. But I have a SMI that can come in here. And it knows that part of the business. And they're experts in that particular field. And it was just an email for me. So that's the reason that I picked Presidio, and I've loved having that I have an army behind me that can help me at every front. And it doesn't matter what part of the network it is, we're highly proficient in cloud, we're number one AWS partner in the country, you know, and we work with Cisco heavily and Palo Alto is heavily on the cyber side. So just a lot of great relationships. And that's one of the things that I enjoy, I don't have to give homework, I can handle all of it, if you want me to if you need me to. So it's a great benefit. I think that harkens back to your days in service, right? Where you guys just did it right? You found the right guys, and you guys rolled your sleeves up and you fixed it. Yeah. You know, I'll pass this on to somebody else. One of those things I know that we've talked about before, David, when you come out of the military, and you're situationally aware, and you have a different lens than folks that just you know, were in their basement gaming and discovered hacking, and ever you know, that they could make some money if they started working for the good, that kind of thing. You come at this with a whole different lens, right? And like you said, You even were thinking about and went into physical policing for a while. And yet it's funny because I come from physical security as well, right. So as a PI, I look at things differently than my husband who is you know, quite the intellect and who's an amazing thinker. But we come at things way differently. I think we make a great couple that way. Because, you know, I helped them with the physical piece in thinking like a bad guy. And he's got all these lovely solutions and these architectures and ways of thinking things from top down. And so I think it sounds like that you're working for the perfect company, because you get to put all of those gifts all in one place. Yeah, I feel that way. And you make a couple of great points in the Marine side of me, right? The Marines are also uniquely positioned because they're the force that can see the airline and see, right, so you got other branches, the Air Force, they don't specialize in that. But Marines that made it a point to specialize in every aspect. And I do bring that to the table. And that mission accomplishment piece, I think, is the other part of what you're mentioning, and just understanding that you can have a full sight picture, full sight, alignment of Battlefield, intelligence, everything that goes into how you attack a problem and take that 360 degree approach to protecting something that comes right out of the basic skills and fundamentals on battlefield intelligence and how to put a battle plan together. So I do bring that to the corporate world, which I think at the beginning of my career, and may have been just a little bit too aggressive for corporate America at that time...

T **Tamara Shoemaker** 06:08

When I went into academia, they were like, what's wrong with this woman?

D Dave Trader 06:12

Yeah. So for sure, I've definitely calmed down over the years. And it's certainly reflected. But I have board conversations. And I like to transact at multiple levels in historically, especially in the recent past. That's the conversations I'm having. I'm having C level and board level conversations, and we're talking about strategy. But I also love the analytical part where I can talk to that security analyst and I can say, what are you doing today as a CISO, I used to do that I would just sit with the analyst and say, What are you working on? And by the way, what barriers do you have? You know, what's in your way? What can I get you? What tools can I get you to do your job more efficiently? And it worked like a charm, right? If he's got seven people or direct reports standing behind them, that conversation can make them feel uncomfortable, because the next time I have it, they've already removed the barrier. So it's a two edged sword all the way around?

T Tamara Shoemaker 06:56

Oh, absolutely. ...All the excuses. But the other piece is because you have the knowledge. And of course, that's what we're trying to sort of bake in with our master's degree program, right? You were at one time those boots on the ground. And so you know that there can be things that are preventing really good people from doing the things that they need to do. And so they're not getting the point ahead of the boss, who's asking them to do the impossible. They're getting someone who sits down with them and says, Okay, how do we make this better? What are we doing right and wrong, and let's get through this together as a team, write that down. I think that comes back from your military background, again, you know, that whole team mentality and that way of, you know, making sure that your forces have everything that they need, right. And we need to think about that that way a lot, right? In this thing, right. I mean, one of the things that I think we run up against and I think that you were talking about Presidio that you don't have that problem, because they offer all of the services and all of the solutions, is that we get very stovepipe, right? And the solutions look like what we ever we are the expert in than what it actually is, right? And so if you have that group mentality of looking at it from a lot of different angles, you're much more able to come up with a multi pronged solution that's going to maybe hold the enemy at bay for a tiny bit, you know, yeah, nothing scares me more when someone says, Oh, I got this. I want to say, Oh, my word, you have no clue.

D Dave Trader 08:17

Yeah, I'm the same way I frequently will tell the customers that I have is if you've got somebody that thinks that they've got this problem completely beat for they try and pretend that they've got some type of advantage, you can't do that. There are no guarantees in this. And you have to think about this way beyond the teenager in the

grandmother's basement with the hoodie. That's not what a proper profile of a hacker is today. These are organizations with departments, and they have their own C levels, they have their own helpdesk, they have their own operations and cloud operations, and you're up against a sizable adversary. And depending on who you're dealing with, I've seen it and I think we just need to get that out of our head that what we're protecting against is someone who's going to accidentally tripped over an open port on a firewall, that's just not what we're gonna see today.

T Tamara Shoemaker 09:01

Like he said that his news hasn't gotten everybody's attention that this is multi pronged attack, and a war to get our information to get our finances to get all the good stuff that we have all of our crown jewels, as Dan loves to call them, right. If we keep going into it the way we've been going at it, it's definitely not going to be a good thing. But I think there's an awful lot more folks like you now in the field, that are thinking about it the way that you are, what are some of the active threats that are prolific right now? It's definitely a new world we're living in. And like you said, these folks are pros. Yeah. I mean, they're trading longer and harder than we are. They're organized better than we are all that kind of good stuff. What's out there that we need to worry about? Are they thinking about at least?

D Dave Trader 09:42

I'm seeing there's a draw to this side, even when you go down the path with a full intent of learning how to defend against this, there's still a draw, there's an interest, you know, there's a curiosity as to what can I get my hands on and it's a tough thing to resist, but there are laws in place. You have to realize, you know, the environment that you're in, I'm seeing here everything from pretty much any attack that you can think of is available. You can purchase these as pre packaged. If you're writing your own code, you basically can sell this and auction these attacks off. These attacks also come with quality assurance, meaning they you can buy them, Wait!? They have a guarantee? they give you a guarantee based on the security that the company has. So let's say like a company has Symantec, they've got a version of the attack that's guaranteed to pass, you know, step 12. So 14, you know, whatever the the particular AV happens to be on the endpoint, there's app stores out there on the deep web that are specifically focused and targeted and on this. So it's just changing the mindset of what people think about when they think about these organizations. But, you know, the most damaging thing that I'm seeing out there today is is ransomware. And then that takes you down a path of talking about business email compromise, which is the number one attack vector, right, the user clicking on a link and opening up a command and control. That is still the number one way and I have a red

team. And I sit on our critical incident response team for Presidio, and I get those phone calls from most CIOs that are like, I'm locked up, hair on fire, I need your help right now, get here as fast as you can. And really, I've seen 50 60% of the network tied up before we're able to start cutting cords and say, you actually have to physically disconnect from the internet, you're completely compromised. And we have to stop that proliferation. Those attacks are so damaging, I mean, businesses can close over this. And I think that that's something that everyone needs to understand is I know that security is not your primary business. And you're going to need some help and bring in some teams and maybe some managed services to help augment a small team if you have it. But you really have to focus on this, it has to be because if you're out on the fringes, and you think you're hiding from this problem, you're not. They're gonna find you. It's just a simple port scan. And they're doing that everywhere. So what are they all sudden pop up on the radar is not having the right setting, or they'll see something that that makes you vulnerable. And they'll say, okay, we ran that play three months ago. And these are automated scripts, it doesn't even take manual intervention anymore. So the idea of we don't have anything hackers want, I've heard that, you know, that's complacency. And I'm trying to get CIOs and CFOs, to realize that complacency model and thinking that you can hide from this issue, that'll get you so far. But that's not a strategy. So coming up with what we can do to to work on that it's been just something I do every day. So I call this left and right, a boom. And I get that from the FDIC. So Academy. And you know that from an investigative standpoint, and how they do mass casualty investigations, it's just how the bureau does that. But boom, is the incident, right. And I always say that boom, is some type of security breach, or I quantify a security breach as exfiltration. So as data leaves an environment, pretty much at the data stays in the environment, I will typically say that's a security incident, but not necessarily a breach. And that gets us into some language around GRC and governance risk and compliance on that side. But I have a lot of conversations that are right of meaning after the incident, and the toothpaste is out of the tube, and we're trying to put it back in there, we're trying to recover. And we're going through triage and stabilization, getting them recovery, and we're estimating blast radius and what's affected. That part is not as fun for me, I like helping people when they're in an emergency situation, and you're trying to help them recover. But you're also dealing at that point with 10 X of investment, right on the other side of that conversation left, boom, you're having conversations on preventative, and you're being proactive, and you're getting ahead of this. And that's when your dollar you can get $1 for dollar, you know, the dollar goes a lot further on that side of the conversation. Whereas there's just so much baked in with cyber insurance, and cyber insurance doesn't cover everything. You've got to bring in a cyber legal team so that everything you're doing is covered under confidentiality, and attorney client privilege. There's just so much that a lot of people don't think about. And so what I like to do is just propose a tabletop exercise, and just say what if this happened, and just mock step through it just to start the wheels turning? And then

of course get granular on what controls are in place? And how do you stop something like this, there are best practices to stop these things, you know, for I always say 90 to 95%. If it's state sponsored, I'm not going to tell you that I can stop that, right. But there are things that we can do to stop the other organizations, the organized crime side, we can just make it more difficult. And it's the old adage of how do you run from a bear, I don't have to be fast in the bear. I just have to be faster than the person next to me. A lot of that philosophy does go into making it just difficult enough for the hacker says, Okay, I'm moving on to the next target, because it's a target rich environment. Absolutely. And I mean, you talked about the fact that, you know, these kinds of things can close businesses. So I've read that in small and medium businesses, one in four, getting ransom attacks will not be in business at the end of the year. Yeah.

T Tamara Shoemaker 14:28

I mean, so I mean, it's having true impact on our economy and our growth. And I like it too, because we go back to what you said earlier about the fact that the number one vulnerability here is the user. It's a cultural thing, right? Like you said, we think that we don't have what they want, so they're not going to get we don't have crown jewels. I'm just a florist. You know, I'm just some small corporation that you know, makes a widget and who cares about that? And it's like, No, you have a bank account right? And I think they're especially counting on even with the small In many businesses, they're doing quantity, right. So even if they're not getting big, big bucks out of you, it adds up at the end of the day. And so it's a cultural thing with our employees and our people. And it's why I went to the K through 12 thing. You know, I really feel like the minutes those kids have any kind of electronics in their hand, they need to know that there's security protocols that they need to take, just like if they're going to operate anything else they get in the car, they know they put on their seatbelt. I wear that one out. So I use that. So I feel like you go on the internet, you know, you got to do a certain things to make sure that you're safe. And then if we bake that in early enough, I feel like that's going to help us along the way, right. So even when these kids are coming up with all this lovely innovations that they're coming up with, they'll already be thinking security... Rather than snapping it on. And rather than having to get consultants like you guys to kind of think about it after, like you said, the toothpaste is already out. You can't get it back in. And like I said, my hair's on fire! you know, and it's like, well, what could you have done? maybe not have that happen? If we could go back there and see how maybe we could have prevented those kinds of things. I think that's a truly important service right now. And I still think as much as we've got things going on, and as many things that are in the newspaper in and and then I still don't think people are taking it as seriously as they should. I mean, is that just me, because one of the things I fear is us that are in this piece are talking to each other. And it's an awesome them, those that are in it, and we get it in those folks that aren't. But basically,

that's why I want this podcast to put this together was to be able to say things to general people who this isn't their thing. This is still important for you, and what can you do to help not be the victim? Right? And so like you said earlier, these are tasks are becoming more organized. They're more systematic, they know exactly what they're going after, again, they can go into catalog, right? I mean, you can go out there on the web and just say, Okay, this is what I want to do today, you know, and some of them are doing it for profit, and some of them are doing it for fun, just to see what they can get away with. And like you said, I don't feel the ones that are doing it for fun, quite as much as the ones that are disorganized. But how do you see some of these things going down? As this increases? And it gets more sophisticated? What are we going to do?!

D Dave Trader 17:08

Yeah, I really like your safety analogy with the seatbelt. And starting at a young age, I think it's so vital. Because once we get into the privacy conversation, and children and the exploitation of so many things, the part of the web that is uncomfortable for everybody to talk about right, preventing that and watching out for that and investing in ways that we can police that everyone's behind that, of course, and coming up with ways that we can stop that type of activities is certainly something that we need to bake in. And we need to teach our kids how to be safe online. And I think you have to start in those young ages. They talk about you know what a stranger looks like online and different aspects and how to stay safe online, but also just how to defend the device that they're on in and of itself on the IoT side. So we're talking about the actual device? And what does that look like? What should they turn on when they get in the car? Right? Where's the seat belt? How do I click it when I get in the vehicle? You know, what's a VPN? How does that work? And how do I set that up? And why is that important? I think one of the things that I struggle with is I try to come up with a less abrasive word than complacency. And I've also been told that I blame the end user too much. And I know that we have to partner with the end users and I have a responsibility. I'm an end user, just like everyone else. I've got a responsibility to know my system that I'm logging on to and I need to know what the policies are and what I'm allowed to do on what systems and where. And I think that complacency is the best word that I've found for it so far. But there's also a lack of Okay, what do I do? Yes, I know, a VPN is good for me. Do I need to turn it on every time I grab my device? grab my phone? No, shouldn't that be out yet? How to set it up properly, so that you're utilizing encrypted communication so that your phone calls and everything else? It's two way encrypted traffic? And that goes back to what we used to do in the Marines and department defense. Same thing, you need to have that because it prevents a man in the middle attack. It prevents clear text, there's no we're not picking passwords out of the air. Yes, that's possible. Yes, it happens. You know, I've spoken at blackhat. I've seen them do it to the wall of sheep out there in Vegas. Yeah, you have to have very simple things that are

even free, you should do some due diligence on what tools that you deploy on any device. But there are good ones out there that are effective, that will protect your data. And you should also be careful of what you're allowing on those devices. Don't just click Allow, as you get the device in your clicking through just granting access to everything, including location. And I think again, we go back to the K through 12 space. And some of the social media apps between Tick Tock and Snapchat, the social interactions are great, and how they network with each other. But think about that from a predator perspective. It's a target rich environment, if everyone's just clicking through, and you know, here's my location, here's access to all my photos. Here's everything that comes with, you know, how personally your iPhone devices and how prolific they are into what you do on a daily basis, but also how much data we entrust in that device. You give away, let's be honest, right. ...Just giving it away. I mean, used to be people had to actually pay for it when, in fact, I think sometimes we're paying for it to give it away, you know, when you draw on some of those apps, you know $3.99 a month. Oh, okay, no problem on that one. And then you realize that it's a flashlight app, and it wants to know your location and all of your contents. Really? Why? Why would you have to have that stuff. So you just paid for them to have access to all that. Yeah. And I think that as a society, we need to actually hold those app stores accountable, right. And I know Google Store in the Apple App Store, they do a good job, they've done kind of a calling where they've taken out, you know, 100, or 1000 apps at a time to have some of those things. And they're doing a better job of how they acquire apps and what it takes to pass through some of their quality assurance testing. I think that's really where we pay attention there, you're always going to be able to go to a website and do a drive by and download something that's always going to happen, but where the majority goes to the well to get those applications, and you can step up security and scrutiny on the screening side, before you're allowed to post something like that into the App Store. Because that particular app, you're talking about that flashlight app that was available on the Apple Store for a long time before they actually figured out how to pull it down. You know, it's a learning experience, but just raising awareness that that it's out there, and this doesn't just affect K through 12. It's great to get habits to those early on how to be secure, and how to maintain privacy. But on the other end of that, there's certainly adults who have not had their entire life on technology that have adapted this over the years that didn't pick up the right habits as the technology came out. I remember 1994 I remember when the internet came out, you know, the children today are like, What are you talking about? Right? We date ourselves. I know, right?

T **Tamara Shoemaker** 21:28

Dinosaurs roamed the earth is well?

D Dave Trader 21:30

I get that a lot too. But as we've adapted and adopted this technology going forward, it's only going to get better. It's supposed to make things easier, right? But it can be one of those things, we have to step through cautiously and just be smart about how we do it.

T Tamara Shoemaker 21:43

Absolutely. Like you said, our users are our number one problem. So we're talking about a workforce. And you know, not the young ones that have had all these things. But we've got a huge amount of folks that are our workforce that again, have that mindset of they're not coming after me. I got an email from Janie. And she says to click on this link. I know Janie. And so I'm going to click on the link. And then poof, my company has now been taken over. Dan and I just watched a couple of days ago, we're trying to look for nicer days, we were bingeing West Wing.

D Dave Trader 22:12

I love them.

T Tamara Shoemaker 22:13

And so there was a thing about how one of the gals Donna decided to email all of the assistants about the calorie count in a muffin. And it ended up it created a DOS attack because the system now this is a while back, right? The system couldn't handle that many emails back and forth from everybody. But I mean, clearly our users don't know. Right? And it is behoove us rather than, you know, user shame. Educate, right, embrace Sure. And to make it easy enough for them to be able to grasp it. And to understand it. I mean, that behooves us as security people, though, right, to break it down so that it's nice and easy and understandable. Are there any suggestions that you as somebody who has kids, wife, parents that I'm sure your tech support for, and, and and right out there that you that you run into and not the major major corporations that you're keeping from being lit on fire, but just one of the ordinary kind of things we need to be doing? So that you see a lot out there that you're like, huh?

D Dave Trader 23:14

Yeah, so I would certainly love to have a zero trust conversation with that group of people you just mentioned, but it's not really practical, right. So at the enterprise level, they're they're certainly different types of conversations between ..., and you know, what's out

there and what's available and how to go about best practice and heading down the ... path in a soar conversation to make sure your operations looking good. But most home users and you know, family members are not going to have that. My house might be you know, a little bit different. Because Because of what I do for a living, but the simple steps.

T Tamara Shoemaker 23:42

You know Dave, because you know, there's a lot of house painters that don't paint their house. And so it would be scary to know how many cybersecurity folks don't actually secure their own stuff. Well, yours is cool.

D Dave Trader 23:52

Well, we talk about shadow IT a lot too. And that's at the enterprise level, we've always been concerned about shadow it because people are using personal devices and BYOD came onto the scene A while ago. And think about what COVID did inverted the entire model, right? So now shadow IT, you could be on it right now, you know, because you're utilizing SaaS based applications. And you're talking back to the data center, maybe through VPN, maybe not. And since I don't own the device that you're on, what type of visibility do I have? And really, where can I insert that and get that visibility? So that's an enterprise conversation, you know, to your question on the family side, I'd like to make sure that I have asset control, meaning I like to know what assets are on the network. If I'm providing you know, an internet service or Wi Fi, I'd keep a check on that. There's a lot of open source tools, which is also free. These are open source tools that you can run on your home network. And if you even if you're not tech savvy, the most basic thing that you can do is run a virtual private network have a VPN on the devices itself to get that dual encryption. And there's simple ways that you can put things out there to kind of mask or cloak your home network, and that's in the DNS on the router itself. Instead of just taking the basic steps of accepting whatever your cable company Your Internet Service Provider gave you as the default settings, there's some things that you can do on there. Especially, I can't tell you how important it is to change your router password. A lot of people just say, Okay, I've got the password, and it might be on a sticker on the back of the router, or that might just be the default, which used to be very simple and available online for anybody to be able to now get into finding your public IP address, because it's listed on every email you send from that location, right, so you can get that out of an email header. So there's a lot of things that you can do, I would say just the most basic of the basic right is make sure you come up with a complex password for the home router, at least, right and make sure that if there's any type of content filtering, do that enable some of those security features. And if you're worried about productivity, or throughput, or efficiency or an increase in lag time or latency, don't be, it's not a noticeable difference. Security is not going to slow

down the connection and you're trying to squeeze every ounce of bought out of the turnip that you can, you have to leverage security even on the home side and have some type of MDR EDR endpoint detection and response, you know, having some type of antivirus, we used to call it antivirus today, we call it endpoint detection, having something that doesn't have to be military grade, it can be just something that works for your devices, it's worth the investment to have that visibility and to know, okay, something's wrong on this particular device in the house. I think that that's just a smart way of going about it. Again, some of those anti viruses even come with VPN that you can set up and like we said, they're getting better, right? So like in the beginning of virus things, and that he did kind of slow it down, my husband called pigs slow, you know, everything's done in pigs, whoa, this doesn't happen anymore, right? they've, they've really done a good job of doing that. And then unbundling a lot of services in them. And then you have one interface that you've got to worry about. So it really isn't that complicated. I have to be a cyber security person to be able to download a good virus protection that has VPN, and that it does a safe check for internet site that you go to and all that kind of good stuff. And it takes a minute. Not all that long, though. Often How about people who have their password in their login for their things their name, once again, like you said, it's easy enough for an expert to look in your email and see what your IP addresses is. But when you then add your name to it, then what's your favorite pets, and Oh, that must be their password, right? Again, we're oversharing on social media so much that it makes it easy for the bad guys not so easy for you to come up with some great passwords, if you're going to use all those kinds of things that you're broadcasting to the world. There are programs in Kali Linux that will do this. And you can just run a compromise assessment, utilizing Cadillacs and Kali Linux is an operating system primarily used for offensive security. So there's a program in there on the social engineering side, which you can give a username, maybe an email address, and it'll give you the history, it will give you all kinds of information across the web of what it can find. It seems like it's daunting, and what can I do against these types of tools, there are best practices that you can put in place in another one of those would be MFA, multi factor authentication. And a lot of us are used to using that in our daily lives when you trying to access your bank account from anywhere and they're going to authenticate you on an account that only you should have access to whether that be email or they're going to send a text to your phone, they're going to interact with you to verify that it's you before they allow that session to happen. You can do that on your own. There's MFA out there that's available. And you can third party, your Amazon account, you're going to log in to Amazon or your Gmail accounts, you can layer on multi factor authentication, and you get a huge return on investment, especially when it's free. But you also increase your security significantly, by having something like that it takes away the account takeover aspect, or at least you're going to see a bunch of things that are asking you to authenticate when you're not trying to that's a telltale sign that someone's trying to get into your account, right and need to recognize those attempts and be able to stop that.

But that's a control. That represents a control that you can put in place on the personal side, which is pretty simple. But it also has high efficiency and protecting

T **Tamara Shoemaker** 28:49

Oh, we fight some of that stuff so much, right? You know, it's funny how the banking industry and the Amazon accounts and your Google accounts. Now suddenly, they don't let you have a choice anymore. let you decide whether or not you want to opt in or opt out of that. But there's so much shenanigans going on right? Now they make you do it and you get used to doing it and you realize it's not that big of a deal. Yeah, I get a text with a number and I can handle a six digit number. Okay, you know, it's really not slowing me down that much in my life, to enter that six digit number to know that it's me. And it's not some bad guy trying to get into my bank account, or whatever. And so many of these things that we do on a regular basis, like Amazon, our banking, they have ways of doing it and even your like your Visa card has same kind of thing where you have to put in that other identifier in order to actually use your card online and next. And that's all free to us as consumers. It's just getting us used to doing that and thinking that way. And again, like you said, we don't want to shame them users and we don't want to do Stranger Danger, so much so that people prayed and also hate us in cybersecurity people, right? I mean, oh no cyber security people are coming at us. They're gonna say no to us on everything that we want to do, because we truly want to enable this right that's The heart of the cyber security person and we love the technology. We love all this cool stuff that's out there. And now we just don't love the fact that bad guys can use it against us.

D **Dave Trader** 30:09

Yeah, I completely agree. cybersecurity used to have a reputation of being the Office of No, right, we were just going to come in, shut everything down. And here's your restrictions. And no, you can have this. And I think that with the onset of dev sec Ops, and being able to get into the operation side with how we're handling development and getting into some coding, and really, it's just about on that side allows to think of security as another quality check, right? Is this secure, and you wouldn't put out bad code that didn't function properly? Well, security needs to be a core aspect of how you evaluate your product. And that starts down at the assembly code level. And we bring it all the way forward. And I know as a CISO, I certainly had to say no, and hold my ground quite a few times. But I love the technology. I love learning about this. And I want you to be able to get to your end, state, your end goal, what you want to deliver. And I just want you to be able to do that securely and safely and make sure that we're protecting anybody who's going to utilize that tool and protect their privacy at the same time. Tall order right? That's a tall we're in there's a lot that goes into that.

T Tamara Shoemaker 31:06

Like we talked offline before we got on and we were talking about job protections. I mean, this career field is wide and deep. And there's so many different areas to it. And it's not going away tomorrow. And we need more folks that are involved in it. But I mean, I think that talking about it in in sort of layman's terms and talking about it as a career path that is not just real, real narrow, because like you said, everyone thought you're going to be the bad guy and losing the company, right? I'm going to be the no guy. And it's like, No, I'm gonna help you, with your innovation. make it even better. Because like you said, No one wants to injure somebody, no, in any way, right? You want to be making their lives better not works. And so now that's where we are. And it is a cool time. But I can't get the word out enough, right? You know, and I love your background, your background is so cool, and so vast and so different. And you have adapted and moved through from the military and getting served. So you're clearly a life learner, which is, again, something that this area needs, because it's not stagnant. Some people say, Oh, well, gosh, I don't want to have to keep learning things. And now I'm the opposite. Please let me keep learning things. Because the minute I stopped learning, I'm dying, I'm bored to death, and I can't stand it right? Find something new to do. And this field does that. And I've seen you reinvent yourself over here. And it's been quite the journey, would you do it any other way. I mean, you know...

D Dave Trader 32:27

When I got into this, and I don't want to date myself, either. But when I got into this, there were two separate paths, you could choose computer science, or you could choose criminal justice. And depending on the path you took, maybe you could augment law enforcement at some point, if you weren't on the computer science side, but law enforcement, you know, badge, gun, patrolling and getting into the detective work and doing investigations, I always had that. So I went to a police academy and got all that training. And then I didn't expect to see the paradigm shift or the convergence of those two things. And not just the convergence, but even the takeover on the technology side today, utilizing key components of any investigation. If you're a detective, and you don't have the technology side down, you can get to the information so much faster to help solve these crimes. So I get to two, two of the passions that I love, and being able to help out law enforcement to be able to even from a messaging perspective, and letting them know that federal law enforcement in the Bureau, they want to work with these companies and want to work with these individuals, and they want to help, you know, one of the stats that stuck with me from the Academy is 80% of our critical infrastructure United States is privately held. Well, we're not a communist state. So the Bureau is not going to just storm in and say you know, your critical infrastructure, we're gonna take the invite, it's a partnership. So they've invested a lot in that public private partnership and

the Office of the private sectors that they have. And everybody's also got this misconception that if you need to work with the Bureau, they're going to show up and re jackets, and they're going to be in your conference rooms, it's going to be uncomfortable. It's not, they're the epitome of professionals to work with. They sit down with you and just like another C level executive on an advisory panel, they come in, they know their stuff, and they know how to help you. And you'd never even know that it was the bureau unless they happen to tell you. They're just highly trained professionals that come in and help. And that's one of the things that I like to always talk about is this, I'd like to change the conceptual a little bit because at some point, you're a victim of federal crime. If you've been the victim of some type of insurgency into your network, that's a federal crime right out the gate right off the word go. So understanding that that's the hat that they put on and they come in and they help you it just like if you're the victim of any other crime. So I like seeing that the technology side even though I chose that side, second, I like seeing how interweaves and interchanges with two passions that I have. And to your point, there's no silver bullet, right? We're going to be doing this and I'll be doing this till I'm 90. And of course I hope sees others follow. That's the reason I also like to help with that. And I know that Detroit Mercy is doing a great job these days, helping converge that as well. I've been reading about what you guys do on the education side, and you're providing students with the ability to not have to choose between those two paradigms. You're saying there's a passion to both you can do both. If you love technology and your investigator, well, we need both of those in one person, let's do it, then you're training towards that as well. So I've been just fascinated and really love what I'm seeing come out of there as well.

T

Tamara Shoemaker 35:11

Yeah, we're pretty excited about that. Speaking of education, you're doing a little bit of teaching on the side as well.

D

Dave Trader 35:18

I have been trying to do some adjunct as well/ What are you doing this from one in the morning? Yeah, I can't really get to it anyway. Yeah, I know, I try and drop in at least this semester, if it's more of a guest speaking than it is adjunct anymore, because there's so much going on during COVID, we've seen an uptick in the attacks that are happening across the board. So I'm so busy putting out fires are typically I can't really get to the adjunct side, but I do love it, I want to help. And I can kill for days talking about this stuff. So you know, what's an hour talking to a group of individuals that want to learn this more?

T Tamara Shoemaker 35:46

Well as long as they're so hungry for the information, right? So I've been working in the K through 12 space, and I talk to these shiny new pennies, these middle school or high school kids, you know, and they're just so excited about about the technology and about the things that can be done, and even some tools and show them the way they're just excited. And I joke about, you know, I should be paying them to have the experience because it's so affirming, right, and I'm sure it's the same for you and is in a different situation than when it's the folks that you're working with. Right, you're not their boss, right. You know, you're just imparting all of the knowledge that you've gotten over the years with them. And it's very cool, because you get to feel what what my husband's been feeling for the last 37 years now. I love teaching and in that in all the books that we get to see and all the alumni that come back, and we wish the older progression that they've had, it's a really cool thing. I'm glad that you're involved in doing that as well, because you have a unique pathway. That's another thing that I like to get out there too is that this is not necessarily a straight pathway. Well, I would love it. If in kindergarten, you started learning cyber, and then by the time you graduated, you were ready to rock and roll and hit one of the colleges, the universities and come out the other end and be able to conquer worlds for us. I mean, keep everything safe. It also can be a marandering wandering path to to get there. Yeah, and maybe not exactly as you expect this, like you said, you went into the Marines and you were very much into the physical policing part. As technology was coming in, almost like my I mean, it's a different story, but almost the same, because now there's a new investigation part. And the internet became hot and listservs. And people on the internet sharing information. And I ended up being able to do way more sitting at the office at my terminal than I could do traipsing all over town trying to find something. And so those paths can come all different ways. And it's because it is such a huge industry. You know, there's definitely something in there for everybody. Right?

D Dave Trader 37:32

I agree. And...

T Tamara Shoemaker 37:32

I mean we're all on one team, too. I mean, even if this isn't your thing, please know something about protecting yourself and yours.

D Dave Trader 37:40

Yes, absolutely. I think that it is key. And it's got to be something that we not only on the

academia side, as we see students progress through K through 12. And having those requirements in getting them to have an understanding of the good and bad side of this, right. Because while the technology is out there, just making them safe on the privacy side is something I think it's incumbent on all of us to make sure that we're protecting the young ones in society. The other side of this is the mentorship piece, I do enjoy that. And I wish I had more time to dive into it. I consider Dan a mentor as well. I like what he's done. I highly respect what you guys have done. And I'm a big fan. And I also feel that responsibility. I'd love to give back. And I hope at some point, I can carve out more time for that it is something to see when you get somebody and you say Listen, this is a good career path and you're really good at Minecraft. Why do you like Minecraft? And how does that associate with computer programming, and there's some great programming classes to get in on Python and some things that we use in the enterprise level in the cyber realm. There's things that we can use and teaching them and putting guardrails around that to make sure that they're doing it safely so that they're operating in an environment where they can't get any trouble. Because obviously, you don't want that. But putting some safeguards in place to make sure that we can teach them and then teach them the other side of it when they're old enough to understand the red team exercises and how those are beneficial for testing and assessment purposes. Instead of nefarious purposes. We can utilize these things as a quality assurance test. And we do that frequently. So I love seeing that. And kudos to you guys. I know you guys have got mentors all over the world, and people who have gone through your programs. And it's got to be fascinating to see that and see what they do with their careers and stuff. You guys have done a great job. So really big fans of your work. And we love the fact that when you came to the Detroit area, you reached out to us and you wanted to get involved right away. And so we've been able to watch you in maneuvering through your career and moving up and up and up and doing all the great things that you do in your space. And you're helping us to protect our critical infrastructures. I mean, there isn't an industry now that's not touched by technology, you know, used to be it was the other way around. It was there was technology, and then there was business. And it's not that way anymore. I mean, even farmers have technology, you know, My son is a crane operator. And it's like just playing video games, right? I mean, with some life and death consequences if his math is not right. And so you know, he's got all these things that you put together out there. So there's nothing that doesn't touch by that. So I mean, you're helping to keep us safe and our infrastructure going and like Dan always says he doesn't want to make friends with the Amish because they they're only Want to know how to survive through any kind of major breakdown in our you know that he's just not made that kind of work? And no he's not but it's a cool place and and I'm glad that you reached out when you did and we got to know you and your family and all the exciting things that you're doing in your career and that you were able to carve out a little bit of time here to spend with us. It's been a wonderful visit we definitely have to the minute we all clear happens we can get together again with

you and Jenny and enjoy a good meal on the boats. Are you counting the days down to when the marina opens back up again? Because I know I always am. I am I just until the sun comes back out.

T

Tamara Shoemaker 40:36

Right? last couple of days, I gotta tell you, me and the old man have been out on the walking trail because actually been very nice outside and like what's going on? And if you live in Michigan, you go Oh, no, what's coming. That's how I feel our timing, but I got those couple of days outside with partially sun and for Michigan. That's great. Good luck for me. I agree. And this partially sunny day with me and have a discussion and I look forward to more of those. And again, looking forward to getting to see you physically, here, Alright, so you take care and thanks so much for spending this time with us.

D

Dave Trader 41:09

Thanks so much for having me.

A

Announcer 41:11

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 SHOEMATL at udmercy.edu. And please plan to join us again for the next edition of the Detroit Mercy Cybersecurity 313 Podcast.