Transcript Podcast 132 Cybersecurity Is a Discipline

May 2022

Tony Covington 00:04
You're listening to the CUES Podcast episode 132.

Tony Covington 00:08
Thank you CUES Podcast listeners for tuning in. As you know, on the CUES podcast, you can hear from a wide range of cross-industry experts discussing trends and topics relevant to you.

Tony Covington 00:19
My name is Tony Covington, I'm the Vice President of Business Development for TalentED powered by CUES. I'm also a former NFL player and have over 20 years of experience in the nonprofit sector with several national organizations. I'm very excited to be your host for this show.

Tony Covington 00:34
With the geopolitical events around the world, we're all hearing a lot about cybersecurity lately. We're hearing that the likelihood of attacks is higher than usual. And we're also hearing that financial institutions are prime targets for bad actors. So I think you'll be very interested in hearing from today's guests.

Tony Covington 00:53
Franklin Donahoe is chief executive officer at Lynx Technology Partners, a cybersecurity consultancy that's also a CUES Supplier member. Franklin has over 30 years of experience in data information cybersecurity, business and technology risk management. Plus, he served in the United States Marine Corps. He also serves on the board of Harborstone Credit Union in Lakewood, Washington.

Tony Covington 01:19
Julian Waits is the senior vice president and executive in residence for the cybersecurity firm Rapid7. Previously, he worked as the general manager of the cyber business unit and public sector at Devo, a cloud native logging and security analytics firm. He also serves as chair of the board of Cyversity, which strives to achieve the consistent representation of women and underrepresented minorities in the cybersecurity industry through programs designed to diversify, educate and empower.

Tony Covington 01:50
So let's get started.

Tony Covington 01:54

Welcome to the show, Franklin and Julian

Franklin Donohue 01:56
Thank you for having me.

Julian Waits 01:57
Good to be here, Tony.

Tony Covington 01:59
Thank you both. We really appreciate it. We're really excited about today's show. Before we get to talking about cybersecurity and how to effectively staff it today, I'd like to help our listeners get to know you both. I was wondering if you might each have a professional quote or mantra that you live by, that you could share with us, Franklin, would you start for us?

Franklin Donohue 02:18
Sure. Thank you, Tony. I guess I would say you know, control what you can, know your limitations and follow through on your promises. Those are really those are really things that I think are important, especially doing what you can that's under your control, not trying to do more influence in areas that you're not qualified to get the help you need. Don't be afraid to ask for help.

Julian Waits 02:48
From me, trust God and integrity is everything.

Tony Covington 02:52
Trust him and everything else will fall into place. And I couldn't agree, couldn't agree more and to the control. I call it "the controllables" Franklin, controlling your attitude, your effort and your output. Those are the controllables and anything outside of that is futile because it will do nothing but frustrate you.

Franklin Donohue 03:09
That's right. That's right.

Tony Covington 03:11
Okay, Franklin, I'd like to start by talking about cybersecurity. First, I'm wondering, why is cybersecurity important to organizations every single day?

Franklin Donohue 03:20
Well, you know, the the world has changed somewhat, but not really, right. We still have people who were robbing banks, but just in different ways. There are still people who are committing fraud, but in different ways. Employees have been stealing trade secrets and communicate, you know, information from companies for a long time. You know, we call it insider threat now as if it's new, but there's always been an insider threat. It's just executed differently. And to some degree, it could be seen as being easier. We have things in digital format. We have people who are sharing information online because they're transacting, not using cash, they're sitting at home shopping on Amazon or walmart.com, or whoever. And they're doing these things, even their health care, that's done over the internet. So I don't

physically have to steal information, but I can I can steal information from afar, and it's far more anonymous. It's important to everyone because we're all affected. The threat actors are more coordinated. Organized crime is more organized, and it's more profitable.

Tony Covington 04:34
Are there any additional factors that can heighten the cybersecurity piece?

Franklin Donohue 04:38
I think the impact to businesses as well as individuals. I mean, I think we talk a lot about you know, there was a breach here reach there at Company X, Y or Z, but real people are affected by this. Their information is stolen. Their bank accounts are emptied. People are filing IRS claims on their behalf and then getting returns that they otherwise would get. Identities being stolen and, you know, credit scores, and livelihoods and reputation can be destroyed. And now we have, you know, modern technology that can make it look as if I am some place that I am not doing something that I am not, saying something that I have not said. And so that type of technology requires us to authenticate and understand people more than we have in the past.

Tony Covington 05:30
Yeah, it's amazing to see it happen on a global scale. But, you know, I think the mom-and-pop situations that happened on a local level, it's the elderly getting attacked with scams on the computer, you know, little phishing things, or they get a new television and an app pops up because they connected to the internet, and all of a sudden, their banking information is compromised, their credit cards are compromised. So you know, and that's just on the local level. So it really is important, to be on point, pay attention to what's going on on a big level when you're talking about banks and such.

Tony Covington 06:06
I've got a two-parter here. Part one, what are some things you recommend organizations do every day to support cybersecurity? And part two, what are some key things you recommend organizations do cybersecurity-wise when concerns are high?

Franklin Donohue 06:21
So I'll flip the question a little bit here. I see cybersecurity organizations, companies, etc., I see them as service organizations to companies. I do get that asked that question in that context a lot. It's like what well, what can we do to support our service here? Well, your cybersecurity function is a service organization. So it's actually two-way but when I look at it from my seat, it's really the cybersecurity technical and others within the IT department and security departments understanding the business, being a good business partner, just not a technocrat or techno speak, or you know, someone who's talking, you know, all the sexy terms and things about vulnerabilities and what happened and how someone could could possibly get in into the environment, but making it relevant, not every aspect or part of the technical environment is equally important, unless, and that's where the technology comes in this world as firewalling or access controls and zero trust and all the things that we like to talk about in the cyber community. What is important to the business? What's important to the customer? What are the assets that we should be protecting in a cost-effective and responsible way? And oh, by the way, there's compliance, you know, there's there's regulatory, you know, you've got the NCUA and

everybody see that's bringing down people's necks every day, not that they're actually, you know, breathing down people's necks, but they do have requirements and for good reasons. And, and Rodney Hood speaks about this quite often in his role, as well as others. So we need to be aware, as security professionals, that we are providing a service that should meet the needs, right, and we should do it in a cost-effective way. Now, what was that? What was the second part of your question?

Tony Covington 08:17
What are some of the key things you recommend organizations do cybersecurity-wise when concerns are heightened?

Franklin Donohue 08:23
I think it's really understanding the issue. I've been in roles where I've had a board member or a person in leadership come and say, Hey, I read this on the internet, how does it affect us or a buddy of mine from this particular company, and then they heighten a concern, which may be legitimate, but we start chasing things that may or may not be relevant. What we need to do is when there is a concern, first of all, we need to identify it before everyone else, which is sometimes difficult, understand how it can apply to our company, credit union, bank, understand that right to the company itself. And then, if we do have gaps, be honest about those things. There can be a tendency to want to not talk about the situation until you have a solution, right? That's not the thing to do. So escalate, communicate what you know, be honest about what you don't know, but have a plan in order to close those gaps. So sometimes, you know, I say over communicate, right? And then people tell you, Okay, that's enough, right? But communicate what you know, be honest about the communication, have a plan to meet those things where you don't have the information and act quickly, act quickly.

Tony Covington 09:43
Do you think organizations are taking cybersecurity seriously or the threat seriously?

Franklin Donohue 09:49
I think it's very much like policing or any type of security whether it's national security or local security. I don't believe that people get it unto til it's in their neighborhood, right until it affects them in some way or someone that they know, or someone in there or a company that's in their industry, right? They don't quite feel the potential of the effects until it happens to either one of those in those areas. So I think they take it as seriously as they they believe that the risk is imminent. And that's where, in cybersecurity what we've done over the years, is we've told these very interesting stories about breaches, and we say, you know that it cost x millions of dollars to remediate. And if we get ahead of this thing, you know, we won't have to deal with this. It's a cost-benefit. But it is oftentimes theoretical, or is viewed as theoretical, because it hasn't happened, you know, my house hasn't been broken into. But if my neighbor's house was broken into, I might get that security system that my wife's been yelling at me about, right. It could be it could be something like, similar scenario,

Tony Covington 11:03
Understood. My grandma used to call it, the same thing that makes you laugh, makes you cry. So you know, you got to be you got to be careful out in those streets.

Tony Covington 11:14
Okay, let's turn to cybersecurity staffing. Julian, what are some things, what are some key things organizations should keep in mind when they are hiring people to do cybersecurity work for them, whether it's a staff member or an outside consultant?

Julian Waits 11:27
Oh, I guess I'll add to one of the points that my colleague was making here, meaning, the first thing is, you know, I'm a big believer, and finally a cynic. He always says start with why. So cybersecurity, as has been said, is a discipline, right? What is it a discipline supposed to do? It has three purposes for businesses, charitable organizations or government entities. First and foremost, it's about protection, and the three things that need to be protected are my liabilities from having to pay money, my reputation, and depth of money from me or my IP. Those are the three things that we cover in cybersecurity. And so if you start with that, the real question is, what's the type of risk we need to manage in the organization? And then from there, what are the disciplines that we need to put in place? And then what are the type of people that we need to manage the risk? The key thing to always remember about cybersecurity is it's fundamentally broken. You know, in this market, anybody who fundamentally thinks they can buy a technology that's going to stop threat actors from coming into your environment? You know, Franklin's exactly right. You want to detect it if you can, but the stuff that you can really detect is only the stuff that's been seen before, or looks really close to what's been seen before? And if that's not the case, then it's all about how do I respond to it and respond quickly enough so that the breach doesn't become material? Because again, every environment, if anyone who's listening to this has a device, and it has ever touched the internet, it is compromised, period. The question is, Is today your day? And so the way you deal with that, is first you protect the things that are most important to what it is you're trying to do. If you're a government entity, you're military, well, first thing I want to protect, I don't want anybody to know what I'm doing before I do. Because that ends up in disaster. Feel people lose their lives. If I'm a bank, I gotta make sure I've got a complete fort around all the confidential information for for my customers, their their identity, information on how to access the systems that they need to get their funds or move their funds around. And then more specifically, their personal information that may not be used to steal from the bank. But all of a sudden, I've got a Social Security number. I've got an address. I've got a birth date. Let me go open some new credit cards now, because as Franklin said, on the internet, anybody can be a dog, meaning, you know, you're just one click away from being able to take over somebody's identity. So to the specific question of Who do I hire? I don't know how you answer that question, right? Because most people I know who are in cybersecurity, and I would say this is the vast majority, never expected to be in cybersecurity. We usually we're IT people or we were governance people or we were doing other stuff. And oh, by the way, you know, gee, we need the security stuff. And it starts with somebody who has a great curiosity. If you're not curious, then you're not going to find the problem, right? Because remember, you can't stop everything from coming in. So the first thing I need to be is aware I need to be I need to be visually attuned to what's happening in my environment and I need to be curious. And then I need to be smart enough to understand you know, if a mature organization, there's some processes I've already put in place. So I need to follow those processes and make sure I can communicate extremely well. One of the most important things in cybersecurity professionals is not technology. It's their ability to communicate, one that there is a problem, two, as best they understand it, what the severity of that problem is, and then three what's the remedy--the action plan we need to put in place to resolve the

problem. And so outside of that, there's not a cookie cutter sheet for cybersecurity people. They need to be smart, curious, and can communicate well.

Tony Covington 15:14
That's very interesting. Because that's not what you think of, you know, when you say, Okay, how does someone get into that space? What ardoe they major in? So yeah, that's interesting. Those are three key things that I've taught.

Julian Waits 15:25
Tony, I was a jazz performance major in college.

Tony Covington 15:28
Understood, understood.

Tony Covington 15:33
All right, I'm interested in learning about what Cyversity does, and how it helps organizations with their cybersecurity staffing needs.

Julian Waits 15:41
Sure, so So Cyveresity is exactly what it says. It is where cyber meets diversity, equity and inclusion. We have been around now for just over seven years. Initially, we were the International Consortium of Minority Cybersecurity Professionals. And the way the organization started is quite simple. A group of us, Franklin was actually in that group, who have been in a cybersecurity field ever since we used to call it information assurance. Frankly, am I dating us a little bit?

Franklin Donohue 16:14
Yes you are.

Julian Waits 16:14
So, yeah, so we'd go to trade shows and stuff. And you know, as it related to women or men of color, we'd virtually be non-existent. And the whole goal was, how can we find a way not to exclude anyone, but to bring more inclusion to it and what drove it more than anything else Tony, is today alone in North America, there are over a million openings for cyber or IT-related fields that support cyber. Globally, that number is well over 2 million. And for some reason, we can't find enough white guys to fill all those jobs. And so we got to go find some other people to help fill in the gap. Because we just don't have enough people in the fight. So it is a numbers equation, and we need to get more people there. And as I stated before, a key goal of Cyversity is to bring people who wouldn't normally be aware or even think of cybersecurity as a place that they can have a career. There are so many different disciplines in cyber. I mean, I can't even enumerate them all. And most of them don't require that you have to have any coding skills whatsoever. So you know, the key thing is, is what we've done in the past, right? And for good reasons. We've always taken you know, really technical skills related to computer. And we always make it akin to mathematics or akin to very analytical skills that you normally have to have. But to be a good cyber professional. You don't have to be an ace in math. What you have to be is curious, smart, able To visualize what's happening in your environment and communicate effectively. That's the

premise for any job, especially those in cybersecurity. So at Cyversity, our whole goal is we want to bring everybody to the park.

Tony Covington 18:03
Wow. So if listeners want to get involved with Cyversity, or hire graduates, what should they do?

Julian Waits 18:08
www cyversity.org. Come see us. We have multiple programs. We're helping people meet, you know, the one of the greatest stories, Tony, that puts me to tears every time there's a woman by the name of Marilyn that I met several years ago, actually out of black hat conference. At the time, she was a retired Army nurse working in a hospital system. And she was she was approaching 50. And decided she wanted to be in cybersecurity. She's now one of the senior people in the cyber staff in the same health care facility where she used to be a nurse, and she's in her mid 50s. And so this is the point about, anybody can do this as long as you I mean, you got to have a goal, you got to have a focus. And then what we provide most importantly to people, other than education and scholarships, is mentorship through Cyversity. People like Franklin have provided mentorship just like they did, as you mentioned, with one of your family members early on. A key component to what we do every day is we have to remember that we have to pay it forward, not just for the next generation, but for those people who also sit next to us who can get in this fight and help go against the threat actors.

Tony Covington 19:18
Wow, that's amazing. I'm a huge believer in lifting as we climb. So thank you for that. Before we let you guys get out of here, we close with a segment called message in a bottle. And what that is, is what is the message that you would leave for your younger self? Franklin you first.

Franklin Donohue 19:37
I would say, I'll try to be concise because I've made so many mistakes. I just wish I could go ... but you know this is a tough this is a tough question. One is I've had a personal and professional board of directors in my life. And those are my mentors that I've confided in to help me personally and professionally. And there's a great deal of, especially from a younger self, we sometimes not all of us are blessed with the humility that we need to get through all of life. We either through lessons, learn that humility, or we never learned that lesson and something happens. But, you know, it takes humility to become a leader. And it takes a great deal of humility to become a mentor as well. You, sometimes as a mentor, you, you realize that you don't know as much or don't have the wisdom or have the answers. And sometimes that's not part of being a mentor is getting the answers but helping someone get to those answers. But I would say, you know, early on, get people in your life that care about your view, your future, and you yourself as as an individual, your development as a human being, and your development as a professional.

Tony Covington 20:33
Excellent, excellent.

Tony Covington 20:36
What about you, Julian?

Julian Waits 21:03
Embrace love. Learn to love when people care for you and they give you great advice. Learn to love when you make mistakes and you can learn from them and move forward. And most importantly, learn to learn enough that you can share everything that you've learned with someone else, as you start from that early life going through.

Tony Covington 21:23
Hmm, giving yourself some grace. Like goodness.

Franklin Donohue 21:28
That was great.

Tony Covington 21:29
That was that was absolutely phenomenal. And and here here on the mentorship piece. I didn't get my first mentor until I was 50 years old. And was that me? Or just, you know, my grinding nature to just try to figure it out on my own. But I was thankful for my first mentor and a couple of mentors that I have gained since then. And I'm like, man, I really went about this the wrong way. I sure wish I would have reached out to these individual.

Julian Waits 21:54
We offer life, you know.

Tony Covington 21:57
Well, that's awesome. Well, thank you both so much. This has been absolutely wonderful. Thank you both for being on this show. And we look forward to...we have to do this again, gentlemen. We have to do it again.

Franklin Donohue 22:09
Absolutely.

Franklin Donohue 22:09
I would love to, just not with Franklin.

Tony Covington 22:12
Wow.

Julian Waits 22:14
I'm sorry. [laughing]

Tony Covington 22:19
That's awesome. Well, thank you both. We really appreciate you.

Julian Waits 22:22

Alright, God bless.

Tony Covington 22:23
Take care.

Tony Covington 22:25
I would like to thank you, our listeners for taking time out of your busy schedule to listen to today's episode of the CUES Podcast. And many thanks to Franklin Donahoe and Julian Waits for sharing such great perspective.

Tony Covington 22:39
Links to the websites for links technology, Rapid7 and Cyversity plus shownotes and a full transcript of this episode can all be found at CUmanagement.com/podcast 132.

Tony Covington 22:52
You can also find more great credit union-specific content at CUmanagement.com.

Tony Covington 22:58
If you liked this podcast, you may be interested in learning more about First Line of Defense, a fraud prevention education program offered by CUES. Check it out at cues.org/firstline.

Tony Covington 23:11
If you're a CUES member, you have access to invaluable membership benefits to further enhance your development. Many membership benefits are available virtually. Make sure to visit cues.org/membership to learn more.

Tony Covington 23:26
Very near and dear to my heart, TalentED, powered by CUES, works with nonprofits to develop the leadership potential of their executive teams, board members and staff. Learn more about the TalentED offerings at talented.org

Tony Covington 23:40
Thanks again for listening today.

Tony Covington 23:42
CUES is an international credit union association that champions and delivers effective talent development solutions for executives, staff and boards to drive organizational success.