Michael Roberts (00:09):

Welcome to the Health Connective Show. I'm your host Michael Roberts, joined by our COO Justin Bantuelle. Today we're talking to Terry Ziemniak. Terry is a fractional CISO and partner in TechCXO's Product and Technology practice. He has over 25 years of experience in the information security field, including 10 years as an information security officer for large multi-billion dollar healthcare organizations in the US. We've discussed all of the different cybersecurity requirements for medical devices in previous episodes, but today we're gonna be talking about how medtech companies can really use cybersecurity as a business driver and a key feature of what they offer, rather than just something we have to do that happens in the background. We'll also look at some of the common ways medtech companies may be missing the mark with security and what they can do to improve on that front. So Terry, thank you so much for joining us today. We're excited to have you here. Yeah,

Terry Ziemniak (01:00):

I'm excited to be here. Thank you for the invitation, Michael.

Michael Roberts (01:02):

Absolutely. It's our pleasure. So we know that connected and robotic devices have certain cybersecurity requirements from the FDA, which have been recently updated. But how can cybersecurity be a differentiator or driver for business in this space? Because as we were just talking about before we started recording, when I think of it from a marketing lens, I go, yeah, security's good. But I don't think of it necessarily as a differentiator. It's not something I wanna lead with when I think of product

Terry Ziemniak (01:27):

Marketing. That's a good question. 'cause I, I think what everyone realizes that security's not free. That's not free. Why do you wanna do it? And, and, and I'm reminded of one of my, uh, earlier clients when I started with the company and I, I spoke to the CEO and I said, okay, you know, we're all queued up. We're gonna start rolling the security program out. Security's not free. Why do you wanna do this? You know, what's the company's objective here? And she said off the bat, she said, well we need to protect the patient data. It's important to do, you know, we have an obligation expectation. Protect it. That's great. It follows up right behind it with, and we're gonna use it as a sales differentiator. You know, there's a lot of people in the spaces that use healthcare data analytics. We're gonna use it as a leader.

Terry Ziemniak (02:06):

We're gonna talk about to our prospects and our clients and our, our other folks. We're gonna lead with the conversation of cybersecurity and it's gonna be a reason that we're different from everybody else. So in that need and the expectation of the prospects and the buyers even growing, every year it's growing because nowadays the cyber security perspective from these clients in these organizations you're selling to, they're looking at you guys, meaning whoever they're procuring from, as a cyber risk. It's very clear nowadays and it's common phrase called third party risk. You know, if you are selling something to a big healthcare company, insurance, whomever you are a risk to them. So keep that in mind when you have the conversations, and that's where cybersecurity becomes the value add, the differentiator, uh, in addition to, you just have to have it these days.

Michael Roberts (02:54):

Yeah. And I know that we were talking about, you know, you've done some work sort of more on the procurement side. You can definitely see from that angle. How often is that like security angle coming up in the sales process? I mean, how strong a voice is security when it comes to purchasing?

Terry Ziemniak (03:11):

<laugh>? Well, I think that that depends on who's buying. So honestly, some organizations are better at security than others. All of them, pretty much all of 'em are gonna do some level of minimum due diligence. So that's all your HIPAA agreements, your business associate agreements, maybe some kind of spreadsheet of do you encrypt, do you backup, do you pen test? Those sorts of things. So those are all built in. The better organizations, and there's getting to be more and more of them because again, this is a risk to the big organizations. Those more mature organizations are being more thorough and you know, more detailed in their reviews because you see these things all the time that these cyber incidents impacting healthcare organizations are coming again from third party risk. So it's acknowledged, it's known within these buying organizations that doing this transaction is introducing risk to the organization every year. It's growing in importance and, and the more careful review is increasing every single time we go through this.

Justin Bantuelle (04:15):

Do you see any kind of like preemptive shortcuts of that space? Like if somebody is presenting SOC 2 compliance audits or like HITRUST or something, do you see that that like kind of jumps you forward several steps in the review process? Or is that kind of like the still we're talking like baseline?

Terry Ziemniak (04:32):

Yeah, you know, it's interesting that that's been a conversation for a while. So again, as a buyer, I still have to go through a list of, show me you are doing these 50 things. Gimme a level of confidence that you're patching, you're backing up, whatever it may be. And if you have a SOC 2, I just have more confidence you're doing it correctly. And that's really a first SOC 2 is no, is not a jump to the head of the line and and we don't review you. It's just more along the lines of we have higher confidence in what you're doing. Now I am seeing, you know, again, working for smaller companies, selling up to the big guys. I have seen recently one or two where it says you must have SOC 2, you must have a SOC 2 audit or you must have a HITRUST. Now that being said, it, it's not necessarily a deal breaker 'cause it could be, we've got SOC 2 on the roadmap, you know, we're working towards it. It could be part of the, what I call cybersecurity story. So if you're a startup, they're not expecting to you be Fort Knox.

Justin Bantuelle (05:24):

You have to have been around for a couple of years for you to have proven out the full range of it. Right. It's a

Terry Ziemniak (05:30):

That's exactly true. Exactly. You can't be SOC 2, you can't complete an audit unless you have time to go back and, and look at your activity. 'cause SOC 2 is retroactive. But I am seeing, seeing more and more contractual agreements say you will do this, you'll get a SOC 2, you'll complete a HITRUST. So it's starting to be put on the list as a mandatory requirement as opposed to just, now we feel more confident. So I expect that trend to continue. 'cause again, think about it from the buyer's perspective. You're introducing risk, you've got my data, you've got access to my systems, whatever it may be. How do I know you're not gonna blow me up?

Michael Roberts (06:05):

Right. Yeah. There's a line of questioning that I want to go down a little bit later on where we kind of talk about business to business selling, business to consumer selling, all of that fun kind of stuff. But I, I wanted to kind of stick in this risk to the hospital, uh, concept. 'Cause I think that so much of what these companies are trying to do is they're trying to put themselves in the position of the companies that they're selling to of the hospitals, of whomever. They're trying to understand what would prevent a sale from happening. What would keep that from going through? And this is obviously like a major category and it doesn't have to just be a negative that we're thinking about. This can actually be a positive that people can build more trust in their companies. What are some of the other hurdles that you're seeing around these types of compliance goals? What are some of the things that, uh, medtech companies may not be doing well or that hospitals are concerned about that they're not necessarily getting the answers that they want?

Terry Ziemniak (06:56):

Well, it really varies. So end of the day, the, the, the function from the hospital's point of view is what they call third party risk. So they need to have a sense of comfort, you're not introducing risk. The way that comes to fruition, the reality of it is, it's generally gonna be a big spreadsheet. You're gonna have 50 questions, a hundred questions, 500 questions. You're gonna have to go through them. So that being said, basically it's cybersecurity fundamentals. Frankly, it's not really high hurdles, but it is things you have to do. And all small companies struggle with these things. So no matter who your, what your company is, you're gonna struggle with. Do you encrypt all traffic in transit? Not many people do that. And even those sorts of questions if, if you are answering it, you gotta think about the scope. So if the question is an obvious one, do you encrypt in transit? Most people would say, yes, we do. But then I would ask, do you do everything in transit? And the answer more often than not is no, we don't. Because if you have perhaps an application in your application, you have a database connecting to a web server, to application server inside your ecosystem, not a lot of people encrypt for whatever reason that they may encrypt across the internet, which is good. But they're truly not answering the question of, are you doing encryption in transit because you're, you're, it's a partial answer,

Justin Bantuelle (08:10):

Didn't realize the scope of "in transit." Yeah.

Terry Ziemniak (08:13):

<laugh>. So I would tell if you're receiving this big list of questions, I would be diligent and actually here's, here's a big tip for your people filling these out. Make sure you're very clear on the scope of what your solution is and what your company does. Because if you think about, again, from the buyer's perspective, you have a security analyst level one who's gotta look through 10 spreadsheets a week. It's a lot to process. So if you're diligent and hey auditor, when you look at this, don't forget I, I'm doing, I don't know, scheduling for pediatrics and you know, it's cloud-based. I'm in AWS what, whatever it may be. If you set that picture, you can clarify that, hey, we're not pulling all, we're not doing, I don't know, a population health analytics, which has a whole lot of data. You know, if that gets breach, it's, it's a big, big deal. You know, we don't have critical uptime requirements. So I, by painting the picture of your solution to the auditor, it'll make the conversation easier. 'Cause then the auditor may not go down a bunch of rabbit holes if he or she clearly understands what your offering is. So that's one thing I'd suggest off the top of my head for these smaller companies, help the auditor clearly understand what's going on, that will give you a better scores in your assessment.

Michael Roberts (09:31):

One of the other ends of this kind of question is like, okay, I know I need the security, but how much security do I have to have? And is it, you know, really focusing on like, hey, just really painting that picture that's gonna alleviate a lot of those pain points?

Terry Ziemniak (09:46):

Yeah. And the good news, once you see one third party risk assessment, once you get that spreadsheet once, it's about 80% of the same spreadsheet you get from everybody else. So again, it'll talk about encryption and backups and antivirus and whatever else it may be. So it's not unique, massive discovery efforts every single time. And there's no harm if you have a prospect, if you're having a conversation, go ahead and ask them. Say, Hey, can I get your third party assessment checklist? We would like to prepare for it and see how we're doing. If you've never done one before, go ahead and ask.

Michael Roberts (10:19):

Yeah, absolutely. And Justin, I know you've been through some of these experiences before and thinking through like how to get through all these types of questions. So yeah, definitely. Like just interested in your perspective around that as well.

Justin Bantuelle (10:30):

Well, I mean, just so much of this is process based, right? It's sort of, oh, we didn't have that implemented. I should implement that. And then you do. And it's just a routine part of your process. There's an initial lift to some degree, but it's figuring out how you're gonna do it and then you just continue on with that. So I think that's part of also where you get this ability to sell it back out as something you do, you take seriously, we incorporated this and we have it, it's like, of course we do this <laugh>, so you have to jump through a hoop once, but then it's done like it's behind you and it's something you just routinely follow up on. Like so much of this, when we're going through it, it was a HIPAA certification basically. There's no like official one, but there's a group that audits and then gives their seal of approval and it gives you, adds a little bit more like credibility to the fact that you take HIPAA seriously.

Justin Bantuelle (11:25):

Because most of the agreements, like you were saying, it's just signing something, saying, yes, we do it <laugh>. And you really don't wanna be caught saying you did it and then something happens and you can't justify <laugh> why you said that when you had this problem. So there were a handful of things where I, I, I think we were compliant. Most of it was just confirming we were uploading this information to their database so they can be distributed out. But yeah, it's a benefit. Like the handful of things we weren't doing, I was happy they pointed that out so that we could incorporate it into what we were doing. It's something that you should, as a mature, responsible organization, care about. It's not about the bare minimum, it's about commitment to this. This is a very important field with a lot of <laugh> risk and a lot of responsibility and you should take it seriously. So I think so many people think of this as that kind of burden or, oh, I don't really, oh man, we have to go deal with the security side of it, but there's a purpose to it, there's a value to it. I think we should embrace that <laugh>.

Terry Ziemniak (12:24):

Yeah, I would agree. And I, I don't think I've come across many frivolous questions that, they're not fringe things. You know, due to what, whatever the controls may be, these are all practical, pragmatic, hygiene sort of cybersecurity stuff that you should be doing to protect your business. And I would add though, Justin, in addition to doing 'em, small company owner as you're building it, plan on maintaining this.

Justin Bantuelle (12:51):

Absolutely.

Terry Ziemniak (12:53):

So realize if you do backup testing once to satisfy an audit, you should be thinking in your head, well I gotta put a mark on my calendar. We do it every single year. User education, we've done it once. Maybe you should be doing it quarterly or monthly. So you know, whatever you build, maintain. Because again, your future third party assessments you're gonna get are gonna have a majority of the same questions and you're gonna already have that addressed and say, yep, we, we know this is all running. We have high level of confidence.

Justin Bantuelle (13:19):

Yeah. If they ask you like, when was the last time you did it? If you said you'd do it and you're like, oh, three years ago <laugh>, it doesn't look so good anymore. Yeah, yeah, absolutely. Yeah, that's what I really appreciate about some of these organizations. When you engage them as an auditor, you have this like standing engagement where they continually come in, check up on you, make sure you're still following the procedures. So producing that paper trail is just really valuable. Yeah, you don't have to think about it, you just send it off when someone asks you for it.

Michael Roberts (13:46):

Terry, one of the things that I've heard Justin talk about before, and again, I'm not the developer, so I'm the one that gets to sit with all developers and just try to soak in knowledge from them. Justin's commented sometimes on the potential adversarial relationship that can pop up between security and everybody else. You know, just everybody that's like, oh, we gotta do the thing because security's demanding it. Mom and dad said we have to do this now and we all have to <laugh>, you know, comply. How have you seen that play out in organizations, maybe healthy organizations, maybe non-healthy organizations? Like how do you see that dynamic kind of working as you're getting the chance to kind of look into a lot of these different places?

Terry Ziemniak (14:23):

I would agree with your statement that there's healthy and unhealthy relationships between security and the rest of the organization, but the same can be said of any kind of risk management oversight. So to keep finance well managed, you gotta set rules and people have to follow the rules or your finances on the same kind of concept. The healthier organizations and the ones that are have healthy cybersecurity culture are ones where the CISO has visibility, the CISO listens, the CISO gets buy-in, the CISO has visibility and met shared metrics. And especially in the small businesses, I think that were a chunk of your audience, security should be an enabler for the processes in which your staff is doing. So you don't have, a small company doesn't have a big governance program that says, thou shall do this and let's verify you're doing this in a smaller company.

Terry Ziemniak (15:17):

The security program should be, here is the lane you're allowed to function in. And we've reviewed the requirements from our contracts and the regulations and our cyber insurance. We've taken all the outside complexity for you. We've given you this lane. You go as fast as you can within this lane, developer or business folks or whatever it may be. If you go out, if you're hitting the edge of the lane, let me know. We'll have a conversation. So if you design it correctly, and again it's, it's the feedback and the communications, it becomes a business enabler. You can go faster because you don't have to stop and ask all the time there, there's clarity and agreement on what needs to be done.

Justin Bantuelle (15:51):

And I mean, the worst case scenario, right, is when you've built it, you're all the way up to it. You do the security audit at the end and go, oh, this isn't a workable solution and you've wasted a tremendous amount of time and engineered something that doesn't really work. So yeah, like you said, if you're hitting the edge of the lane, talk to me now

Terry Ziemniak (16:07):

<laugh>. Yeah,

Justin Bantuelle (16:08):

Yeah,

Michael Roberts (16:09):

Yeah. I think we've definitely seen that kind of response like we were talking about in terms of setting the rules, but enabling too, I mean, we've worked with some organizations and some very large companies where we're talking more to the marketing folks and legal's reviewing every single statement and reviewing every single thing. And sometimes that response comes back and everybody's just like, oh, they're just trying to keep us down. We're all just sad. And, and I think we see the same kind of thing like on the development side of things. So I love that as an enabler instead of just as an oppressor <laugh>, which I think sometimes like everybody gets the bad title of that sometimes. Yeah,

Terry Ziemniak (16:40):

I, I agree. And I think there's also another, another concept worth digging into is security. And I usually call it a data protection program more than a security program because it's typically you're gonna roll security, privacy and compliance would have some kind of unity amongst all of 'em. But what this function gives you is this is your function that helps you decide how secure you have to be. So these are the ones that listen that get input from, again, the regulations, the cyber insurance from existing contracts. So you've got MSAs and SOWs and business associated agreements that have security expectations. Those need to be accounted for. Listening to your prospects and listening to individuals and listening to internal staff. All those different perspectives of cybersecurity have to be accounted for and built into your program. And that, and that's really what security's gonna give you, your data protection program is, Hey, hey Justin, when you're writing code, you don't have to go read the contracts. We've done it for you and we've translated HIPAA for you, we've had conversations. We all agree for our organization, this is what it means. Here's your lane, Justin, now go as fast as you can. So being able to look at the outside world and define what is secure enough that that's really the big value there.

Michael Roberts (17:55):

Nice. We've talked a lot about sort of this B2B exchange. I want the hospital feel safe enough so that they'll buy my product, but there are plenty of medtech, and I'll just say like digital health products in general, like we'll kind of broaden the scope a bit here where, hey, you're going directly to consumers, you're going directly to patients, and you're starting to have, starting to have those conversations. I am more aware and more concerned about things like privacy and security and all of those kinds of things in the past few years. But I look at things like Facebook and I look at things like people not reading the, you know, agreement statements and I'll fess up that I don't read them all either. And we as consumers and as customers in the United States care, kind of, but there's a lot that we don't care at the same time.

Michael Roberts (18:41):

But how do you advise companies that are trying to reach out to them? What kind of security are, are people putting in place? Like as we're recording this, this is right after AT&T has disclosed that oh yeah, our bad, like people hacked in and got a whole bunch of information from us. So this is something that people are hearing in the headlines every day, and yet we aren't reading the fine print a lot of times. So there's this weird contrast that we have within ourselves in the United States where we're, we're dealing with this, but places like Europe, places like other places like that, that are very, very concerned and really paying attention. So just curious how that, there's a lot of things I've just asked there, but curious how, what your impression is of that sort of direct to patient, direct to consumer models.

Terry Ziemniak (19:24):

Yeah. Well it, it all comes down again to the idea of your perspectives. So what you're adding is what's the perspective and the expectation of a consumer, an end user. And practically speaking, what that translates to is into data governance. So this data set, which is maybe not medical, but it's identifiable information. PII information, not medical, but I know Justin, I know his email address. That information has to be protected even though it's not HIPAA data. Your data governance structure should tag that as PII protected or personal health personal information. And you should have clarity, Hey, development team, if you're working with PII, you will do correct logging, you will encrypt, you'll do X, Y, Z. We will, maybe that data requires after three years, you delete it, you have to support the ability of user. Michael says he wants his data pulled out, how do he pull out?

Terry Ziemniak (20:21):

So again, defining the rules, defining the lanes effectively for this type of data, here's what you can and can't do with it. Developer, you're responsible to make sure this to get done. If you have any questions, let me know. Again, it could be translated in that same idea of we have a structure, we have a lane for you, but it does mean going out, not necessarily security perspective, but a privacy perspective, which is identify your data because well, everyone's on the AI journey journey, so you hopefully have your, your data identified, you have governance concepts, you know all those. You just build onto that and, and use that to take the consumer perspective and roll it into your data protection program.

Justin Bantuelle (20:57):

Have you seen these sorts of products or the marketing out to it, emphasizing that or making that a differentiator to competitors? Do you see that, I guess maybe the consumers understand it to a sufficient degree that that is a differentiator? Or do you think it's more about mitigating the risk of being the next one that leaked a bunch of information you weren't supposed to?

Terry Ziemniak (21:17):

Well, I <laugh> as, as a consumer and as someone who's got, you know, three kids, early twenties, late teens, I don't think a lot of people really care about it. You know, they, they complain when it's breach, but on the other hand, they'll post whatever they can <laugh>. So it's, it doesn't feel like a privacy issue so much as a control issue. I don't care if it's shared as long as I'm the one doing the sharing.

Justin Bantuelle (21:40):

Gotcha. Yeah,

Terry Ziemniak (21:41):

It also kind of lends itself well to these new consumer privacy rules that are coming. Like California, it's very close to how GDPR manages it, that as a user, I need some level of control over my data. You know, you have my whatever information, I wanna be able to request you to update it, I wanna be able to make you delete it. If you're gonna sell it, I don't know, do I get some kind of value out of the sale, whatever it may be. So, so it's kind of, it, it feels more like a control issue than, than a straight privacy play. But honestly, as an end user consumer, I don't think really, no one reads that user agreements <laugh>. No one really cares. I i, if I can save two bucks off my widget and there's a privacy concern, what decisions you gonna make? I, I don't know.

Justin Bantuelle (22:29):

Yeah.

Terry Ziemniak (22:29):

Yeah. I don't think that that shifts the needle from marketing perspective. Maybe Michael, you have a different idea on that, but listen, go and listen. Help your group define that right level of security and privacy by listening to those people.

Justin Bantuelle (22:40):

Yeah. Because I would imagine this is also something, and I've seen this actually come into play sometimes where someone's left scrambling as an organization because they didn't engineer to be able to handle this kind of, uh, like data deletion for example. If you don't build something in upfront, maybe it's scattered across a dozen different data sources and you don't have a tool and now you have to implement this and are you just having somebody go and delete it manually? Are you assembling a tool? How long does it take you to build that? And have you thought about that upfront? You could have engineered this a different way. So, and

Terry Ziemniak (23:14):

You're also seeing more and more of the concept of a, I'm sorry, more and more the idea of the, these safe harbor concepts. If you can show reasonable diligence and you're following standards in your security program, privacy program, then if something bad happens, you can say, Hey, we weren't perfect, but we were making a reasonable effort. I think that's gonna keep bubbling up in this legislation because no one's bulletproof. Sure. Deciding how secure you have to be. Do you need to be a eight outta 10 or a nine outta 10 or a 9.5? Those are really hard things to do. But if you can follow frameworks like NIST has a great one, you know, whatever it may be, there's all sorts of frameworks out there. Following the frameworks and make reasonable effort to be able to document Sure. You're doing it. That will, I think address a lot of least the regulatory risk. It'll address concerns of class action lawsuits, which <laugh> are popping up all over these days. I mean, these lawyers are right behind every single breach that's out there these days. Yeah, sure. Maybe that's what moves the needle. You start suing them enough and, and things will change.

Michael Roberts (24:15):

Yeah. There's a marketing guy that I listen to quite a bit. His name is, uh, Mark Schaffer and his sentiment around privacy things in general, he just keeps saying, thank God for Germany, because they're gonna go, you know, make sure that they like follow up and sue and you know, put <laugh> put push out and to make sure that somebody is thinking about this and these companies are having to review their policies. It is interesting because like I've started using some of, uh, Proton's offerings that they have for like storage and for some of these kinds of things. And it is interesting because there is like a class of consumer that really cares, but it's not a lot in the US It really is a very small market. And so I think you really do start to have to think really heavily. So if you're doing anything in Europe, that's a very high bar. It is a very high bar to to, to have to match. And it's interesting to be in some of the marketing communities that I'm in, and to hear somebody in Ireland coming back and going, yeah, that new Apple intelligence thing that they're talking about getting, we won't have that for a while, but it's nice that it's coming, but you'll just have to let me know how it plays out.

Terry Ziemniak (25:15):

And that European perspective may not be a bad bar for US companies 'cause we don't have a federal rule in any of this stuff. So yeah, California and Vermont are making these really cutting edge statements of you will allow consumers to do X, Y, Z with their data. Yeah. And if you're working out of, I don't know, Florida, you've gotta account for this because what internet based company or healthcare company works exclusively with one state? None of us do. So, you know, understanding the, the, the, the lowest, I guess the highest bar across all the states really becoming effectively GDPR.

Michael Roberts (25:47):

Yeah. Right.

Justin Bantuelle (25:48):

Yeah. And if you already have it because you were concerned about this, then you're not sweating it when these rulings are rolling out versus, oh man, <laugh>, when do I have to budget for this? When's this gonna hit me? Yeah. Mm-Hmm. <affirmative>,

Michael Roberts (26:00):

Absolutely. I live in Tennessee and there was something that came out where I was wanting to see if I could pull my data out of this, and they were like, LOL, you're in Tennessee, we don't have to do anything, you know, because you, you don't fall in one of the jurisdictions that we have to worry about this. Interesting. Are there any other non-technical things when it comes to security, when it comes to how people are just thinking about this and approaching this that you would advise our audience to be thinking about or, and or to consider as they're looking at, at how they're handling these kinds of matters?

Terry Ziemniak (26:28):

Absolutely, a hundred percent. Because, uh, when you think cybersecurity protection, they typically break it down into people, process, technology. You can't buy your way outta these cybersecurity issues. And I'll give you that. One of the more common examples is a basic phishing email. Hey Michael, I'm pretending to be your vendor. Here's my new bank routing information. Please send my next payment this direction. All the technology in the world is not gonna be a perfect solution to that. So your email filtering, the technology is getting better. It was gonna help, you certainly need it, but you've gotta train Michael to be cynical on emails and you need a process that says, before you change bank routing information, you will, I don't know, validate out of band or something like that. So people, process, technology, all of those have to work together. And frankly, there's a lot of big wins and meaningful ways to move the needle that don't include buying stuff, training users, shoring up your processes, people are working from home these days.

Terry Ziemniak (27:27):

Have you modified your processes to account the fact that Michael, Justin and I are not in the same office anymore? So yeah, absolutely. There's a, there's a whole lot there. And again, if you were to work on a, we talked about frameworks, value of a framework, if you were to look at a, a, a solid framework, again, NIST for those are aren't in the know, NIST CSF cybersecurity frameworks a great place to start. It'll broadly talk about all these things and it'll talk about contractual protections. It'll talk about, I dunno, auditing, it'll talk about business continuity, a lot of the non-technical part of cybersecurity, but certainly a value, and frankly, in many cases, more valuable than just buying more stuff.

Michael Roberts (28:05):

Absolutely. Terry, thank you so much. This is exciting stuff. I, I really enjoy talking through all these details and, and I thank you for translating it for the marketing guy and on the call here. So I definitely appreciate it. Thanks so much.

Terry Ziemniak (28:16):

Yep. It's a been a pleasure.

Michael Roberts (28:21):

Terry shared a lot of great insights about cybersecurity today, from how medtech companies can use it as a business driver to common issues that medtech companies face with security. Thank you for tuning in today. You can find Terry Zimak directly at terry.ziemniak@techcxo.com. That's Zim Niac, spelled Z-I-E-M-N-I-A-K. For more on the Health Connective Show, please visit hc.show for previous episodes and more on Health Connective as a company.