Albert Chou:

This is IT Visionaries, your number one source for actionable insights and exclusive interviews with CIOs, CTOs, and CISOs, and many more. I'm your host, Albert Chou, a former CIO, former sales VP, and now podcast host.

Welcome everyone to another episode of IT Visionaries. Today, we have a special guest. Her name is Cindi Carter and she is a Field Chief Information Security Officer at a company called Check Point. According to their website, Check Point is been the 22-time leader according to Gartner for firewalls among other accolades and awards. She has a wealth of experience serving as a CISO or similar role for over 15 years it looks like in cybersecurity. If you want, you can find her at many speaking engagements like The Official Cyber Security Summit and SecureWorld among others. Just Google her name, you'll find her. That's Cindi with an I. Cindi, welcome to the show.

Cindi Carter:

Thank you, Albert. It is a pleasure to be here.

Albert Chou:

All right, let's get started. Just like we do with all of our shows, for our audience that may not be familiar with Check Point, can you give us a quick rundown what is Check Point, what does it do and we'll dive into the industry, your role, and so on.

Cindi Carter:

Of course. Well, our official name is Check Point Software Technologies because really, although like you said Albert, we have been known as a firewall company for many, many years, our founder and CEO, Gil Shwed, is the, some people say godfather of the firewall, but we have so many more capabilities that protect organizations locally and globally with their cybersecurity needs. We cover everything from the network, the traditional firewall and everything in between there, as well as organizations that are looking at a cloud-first strategy and moving operations into the cloud, as well as end user experiences, endpoint, email security. Then of course, let's not forget to finish out the entire lifecycle of all of that, all of the support, the managed detection and response capabilities and things like that that you need to sustain your security operations.

Albert Chou:

For yourself, you sit at this high profile position. You do a lot of speaking engagements. We've had multiple cybersecurity guests on our show. We understand that you have a bit of a specialty specifically in healthcare. What is unique in healthcare that requires a little bit different attention, let's say.

Cindi Carter:

There really are some uniquenesses when it comes to healthcare. I'm just returning from the HIMSS Cyber Health Care Forum in Boston as of last evening, and it was all clinicians as well as cybersecurity leaders and practitioners that we're really talking about how we're solving some of the same challenges that many organizations are seeing when it comes to cyber threats and how to protect themselves, and even more importantly, how to prevent it from happening to begin with.

Albert Chou:

For yourself, give us a little background. What is happening, I guess, you mentioned some of the uniqueness to it. I'd love our audience understand a little bit of the differences and understand what is happening in this field that maybe they may not be as familiar with.

Cindi Carter:

When you think in terms of healthcare and when you think in terms of, okay, well high-tech organizations and many of us, when we think of technology, we think of the Microsofts or the Apples or the Googles and all of those super high-tech organizations, Amazon even, but a lot of people don't necessarily equate high-tech with healthcare, but it's absolutely there. It's been there for several years and it's been there in everything from medical devices all the way to the electronic health record. When you're talking about healthcare, you're talking about people's lives. A lot of us have had focus initially in years past in financial services, because that's people's livelihood.

Albert Chou:

Sure.

Cindi Carter:

And any time a financial institution or financial services organization was compromised with a security incident, that was all over the news, people were losing money, although many of those things are typically addressed, but there's a lot of attention towards that. There's been a huge amount of regulation in the financial space around cybersecurity and everything else in between to protect those organizations and people's investments.

But when you have to think about healthcare, this was back several years ago, but there actually was an executive order that was signed by our government, executive order 13636, write it down, and that actually put healthcare as part of this nation's critical infrastructure along with the other things that we take for granted day in and day out, electricity, water, those utilities, things like the gas pipeline, everything else in between that we rely on a daily basis.

Healthcare was also placed as part of our nation's critical infrastructure, but healthcare has very often lagged behind in being able to put some of those innovative technologies in place and then, of course, being able to enable that in a secure way. Now I think as we look forward, and I know we'll probably talk about this a little bit, Albert, what are we seeing going forward, what are some of those predictions in 2023, the uniquenesses within healthcare are, at the end of the day, the electronic medical record contains the most richest information, the most uniquely identifiable pieces of information about a human being besides their own fingerprint.

Albert Chou:

I've never thought of it that way.

Cindi Carter:

In addition to just the institution itself, the healthcare institution itself, the employees that work there, the clinicians, everyone else that is part of that organization, now you've got people's medical records and think about what would happen if that data were to become compromised. What if your blood type were to get changed? What if the allergy reactions that someone that you love was changed and all of a sudden, they were given something that could be deadly to them? The awareness is there, and I am so

excited about where we are going to integrate cybersecurity into every single clinical and healthcare innovation decision that's being made.

Albert Chou:

The way you just described that is this, and I want to relate to something that's very timely, how critical our society depends on infrastructure and how certain things need to exist. A lot of times you might not recognize it, but if you take it for granted and if it's taken from you, it's very quickly identifiable how dangerous it is.

Cindi Carter:

So true.

Albert Chou:

This happened in North Carolina recently, not a healthcare attack, but there was someone who shot a substation that used gunfire on a substation, which has put basically electricity down in its entire community. There is no way to get these parts in place. One of the biggest things that they said right out the gate, critical infrastructure, was the hospital systems and basically all these people, so it's not even they had a machine, like you said, some people need a machine, maybe you have dialysis, critical medical needs, you might be on lifesaving equipment. But then they were saying, no, they don't know how to treat anything because they can't look up anything, they have no evidence of anything, they don't know if you were to say, "Hey, I want medication," they wouldn't even be able to say, "Oh, you already are prescribed a certain medication, this is not a good fit."

And so, this town in North Carolina is being basically forced to vacate. They can't live there. There is no way to live there. It's from electricity and you just start realizing, to your point, of course you can attack critical infrastructure like electricity, but effectively, like you're saying, your medical record is now, it's critical infrastructure too. Is that happening? I guess foreign agents, are they trying to attack and erase or change this data? Is it just people trying to steal data or you guys don't really know, you just know that people are trying to get data and you guys got to stop it?

Cindi Carter:

Well, I don't like to go too much to the dark side of things, but we do live in a dark space sometimes when it comes to these conversations, but that's the reality of the situation. As I mentioned before, that medical record is rich with information. Think about it, it's not only got your basic demographics, it's got your date of birth, it has your social security number, it has your insurance information, it has that personal information about your blood type or your allergies or what medications you are taking. It also has financial information. You may have a credit card on file to take care of those copays.

It's an easy target when you think about that. There's that type of information that is readily available at those cyber criminal's fingertips, and it can cause, whether they're looking for financial gain or they're just looking to cause disruption, those motivations are different and similar in so many ways to any of the other attacks that happen in other industries. But when you take it a step further and you really think about, dare I say the word, cyber warfare, and you really start thinking about the physical side of it, human beings' lives are at stake now because of what could happen if a medical record was tainted electronically or compromised electronically like that.

Albert Chou:

That makes total sense. I agree. We don't want to over-harp on the fact that that's the reality of the world we live in. There are going to be cyberattacks. People want information. Let's turn into something that, what we can do about it, and which is how do we stop these things. Because one of the things about IT Visionaries, which we are privileged to, but it's also narrow in focus, is that we typically talk to people in tech companies, which probably as a whole maybe have a culture more aligned towards having a secure infrastructure doing more secure things, more people using password tools or 2FAs.

But, what I know about other fields and healthcare is going to be one of them is that that's not their primary focus. Their primary focus is typically taking care of patients, so good cybersecurity hygiene and practices. I'm sure each hospital's got a team or whatever, but that's probably not top of mind for everybody. It's probably not a cultural top of mind thing for all the team members. When you work with these groups or you're talking to these groups, how do you convey how to solve and protect their systems and infrastructure, because like we said, it's not really like their focus?

Cindi Carter:

I was actually on a panel where we talked about clinical perspectives in cybersecurity. When I thought about that, all three of those words haven't been in the same sentence for a long time. Sitting on either side of me was an internal medicine doctor and a pediatrician. We had the most engaging, well, at least from my perspective, we had the most engaging conversation. I hope the audience felt the same way. But it really, to answer your question, Albert, there's a lot of things that we can do now when it comes to really integrating cybersecurity and this technology innovation into what a healthcare practitioner does on a day-to-day basis, and there's a lot to unpack here, so I'll try to be as succinct yet give enough detail behind each of them. But one of them, first and foremost, and I love to use medical analogies, is an ounce of prevention is worth a pound of cure.

We talk in terms in the industry about, well, how do we stop these attacks, or how do we defend ourselves, how do we become resilient? But if we really step back for a minute, when you think in terms of resilience, resilience takes you back to the state that you were before that negative event happened. Don't you want to come back stronger than you were before? You and your CrossFit buddies can have a conversation about that.

I love to have this conversation with folks around going beyond resilience and really doing this thing called anti-fragile. There's a book author, his name is Nicholas Nassim Taleb, and he's the author of the book called Antifragile. While I may not agree with everything that is in the book, I always am inspired by topics like this. I'm always inspired about how can I weave it into not only the conversations that I have, but in things that we can do collectively together.

When he describes that whole plateau of resilience and where, yes, in many organizations are doing a fabulous job of resilience, and I don't want to downplay that, but when it comes to that negative event that happens, that takes your resilience to the core and it tests everything that you've put into place. You may think, okay, well I had my backups, I was able to restore, or we were able to take things offline in time so that no further damage was done, or whatever the case may be, whatever that incident response was, but when you're resilient, it really is the true definition of resilience as you return to the state that you were before something happened. He is all about, in his messaging, about how do you come back better, stronger than you were before, and that's where antifragile comes into play.

I love that because I think that it really does have a lot to be said for that preventative aspect of medicine. We all know we should eat right, we should drink plenty of water, we should get our exercise, everything in balance. I'm a lover of chocolate, I won't deny it. I've got my little sweet tooth and things like that. But do I eat chocolate for breakfast, lunch and dinner? Of course not, because I would probably look like a Mounds bar if I did. Everything in moderation, but that preventative aspect of

medicine, of course, is doing the things that you can do to take care of yourself, take care of your families so that you don't end up having to seek medical care.

Now, we know accidents happen all the time, but look at some of the preventative things that we've done in medicine even since the first smallpox vaccine or polio vaccine was created. That's preventative medicine. That is preventing that from happening over and over again. We created antifragility in our entire bodies by building up those antibodies so that those things don't affect us. That's a perfect example. We could do the same thing with our cybersecurity systems.

The conversation that I was having with these two gentlemen was really all around integrating cybersecurity into everything that the hospital healthcare organization does instead of it being that afterthought, instead of bolting it on. I always say secure from the start. Every conversation should have a security person at the table, not only at the table, but their voice. Not only being able to say things, but that it's heard and it is put into action.

We have to be careful with that though, because there's that concept of security and usability and clinical workflow that has to be considered. Many of the organizations that I've worked with in the past actually hire clinicians on their technical staff so that the technical staff can understand that workflow and that the clinicians can then understand the technology aspects and what a great partnership. The optimist in me, and I am an optimist, I do feel that we are ripe for a lot of really great things that are going to continue to happen in healthcare and how we're going to be able to keep things safe.

Albert Chou:

When you were saying that, I was replaying in my mind when my wife was giving birth and there was a person trying to enter her medical record in, and she's in tremendous pain and frustrated. She didn't want to deal with it. I'm just imagining a hospital with cybersecurity practices where that's like they have 2FA codes and someone's waiting for their code. You got a patient screaming at you like, "Hey, I need help." He's like, "Well, I haven't got my 2FA yet. I can't lock in and do anything."

Give us an example of... That is to me, in my mind I was like, I just came up with that and I don't even know that's actually the problem. But you know what I mean? I was like, if that was true, that would be a problem because we've all been there. Everyone who know has been there where you're waiting for your 2FA code and it doesn't come, it doesn't come fast enough. Of course, in healthcare there's way more high pressure situations where getting access to information is probably mission critical. Seconds are critical. Give me an idea of, you said antifragile, antifragility, it's an easy thing to say. It's one of those things, easy to say, hard to do.

Cindi Carter:

It is.

Albert Chou:

Give me an idea of some things that are being applied.

Cindi Carter:

Sure. A lot of that too, oh goodness, this is a lot to unpack. When you think in terms of the patient care model, think about what the pandemic taught us and the fact that care now moved from the four walls of a healthcare clinic or a hospital to way more distributed healthcare. Telemedicine, telehealth, that took a massive increase over the last two years. People being able to just enter into a portal and then to be able to speak with a clinician or their physician about even a wellness exam or a wellness checkup, or

if, "Hey, my head feels like it's ready to explode, I've got this sinus thing happening," and they go over your symptoms with you and things like that. That distributed care model is also something now that the cybersecurity is right along there for it.

Think when you, as a patient, have to log into that portal, I always think, of course, because I'm in the business that I'm in, but all right, what is behind this me logging into this portal, I'm thinking about is it a secure transmission of me entering my name and my credentials? Is my information going to the person that I intend or the place that I intend for it to go? I once worked at a company that that was one of their... their flagship items was this patient portal. From a cybersecurity perspective, it hadn't been thought about during the software development side of that portal being created, so we had to go back and re-architect a little bit and start really thinking about what does that software development lifecycle look like to embed security in there? Because we can't have an at-risk portal out there in this type of information to be transacted back and forth without putting the right security measures in place.

It took time, I will tell you that. These things don't happen overnight. This integration of cybersecurity into that clinical workflow, and even in this case, this was to an engineering workflow. This was already tech, but it wasn't something that the software developers were used to doing every day. They have to get those code releases or those features and functionality and things like that out every two weeks. Deliver, deliver, deliver. Add value, add value, add value.

And so, we started a process by which we broke down all of the different areas that were involved. We got everybody in the room, everybody at the table, because a lot of times, the person sitting next to you had no idea what you were doing and what dependency or even downstream relationship that you had with each other. And so, we started to talk in terms of, before a new feature or functionality or product or anything is a twinkle in a product manager's eye before that first line of code is even written and before it's released into production, and then you start that life cycle of support around it, we have to think holistically about what are we going to do to wrap all of this with security so that it doesn't create friction.

Same thing with that clinical workflow model. That's where I mentioned earlier, we brought those clinicians, those practitioners to the table with us to talk about what would this multifactor authentication look like for us? What would be an acceptable delay in being able to ensure that yes, you are the right person that is logging into this information to do this treatment, to make these decisions, et cetera, et cetera? I'll just finish with this because I know that we could probably spin off into a lot of different areas here. But when you do stop to think about what are the cybersecurity organizations thinking about in this space, this is where we've done a terrible job of branding this and it's called zero trust.

The reason I don't like that term is because to an end user who may not be technical, who may not have grown up in cybersecurity, it's like, "Well wait a minute, you trust me to do my job. I'm here trying to treat people, I'm trying here to save lives or make their life better, but yet there's this thing called zero trust. You don't trust me to do my job?" But we have to think about this as just trust.

And so, that's where we go back to that drawing board and we talk with the groups that are involved about where does the data come from and where does it need to go to and what kind of data is it and who should have the different levels of access to that data along that data's journey. It's really understanding the business of your data, whether it's healthcare, financial services or anything else in between and bringing the people that are the users of the data, the consumers of the data, the processors of the data, the people that support the data on their journey, bringing all of those people into the room together just like we brought the clinicians together with cybersecurity is really how we're going to make this happen.

Albert Chou:

When I think about the amount of integration that has to happen in a modern hospital system that you're discussing, it's just different. It's fundamentally different.

Cindi Carter:

It is.

Albert Chou:

Let's use some examples for our audience. If you're using a service, let's say you're going to your, let's use e-commerce to start. If I'm a shopper and I shop online, really all I need is the portal to work.

Cindi Carter:

Great.

Albert Chou:

The seller needs to make sure their inventory systems work and their shipping systems work, and that's fine, but a hospital is a collection of devices. All these devices have different manufacturers. They're all collecting data on its patients and across different records. It also relies on the software front of, I would say, the intake software is also a system that knows how many patients are occupying which rooms, which facilities can handle you. Like when my wife comes in, obviously if I need an OB-GYN or whatever, you know what I mean?

You think about all these things that have to talk together, and what I've learned about the healthcare system specifically is like this, you kind of talked about this, let's get together. It's like, there is no standardization. Siemens is going to make their machines one way. Epic's going to make their system another way. It's usually a third party from my understanding like has to come put it together because these hospitals don't actually have people on staff that are designed to integrate all this. For anyone listening out there, hospitals are mostly implemented by a third party. It's not the hospital itself integrating systems. Like my friend Brantley down the street, he's a CrossFitter. He works for AHEAD, but they integrate hospital systems, which I was like, "Well, how many things do you need to plug in?" We're just going through. I was like, "Holy cow!"

Cindi Carter:

All of them. They all need to plug in. That really, I love where you're going with that too. You touched on some of the manufacturers and things like that. When you think about the investment that healthcare organizations have, or even any organization nowadays, e-commerce with RF guns scanning things in, you see your Amazon person drive away, they've taken a picture, they've scanned that delivery. All of those little touchpoints, all of those devices, that internet of things, that internet of medical things, they've made huge investments in those devices, and healthcare especially. You think about an MRI machine, you think about some of the blood machines that the lab uses to separate the plasma and do all the good things there. Some of those things were never intended to be connected to a network. Think about that.

Albert Chou:

I want to add to your story. My friend, he owns a forensics engineering company and they actually do accident reconstructions to figure out like could this have happened or not. He has a CT machine and I

said, "Well, how much is a CT machine?" He said, "I bought it used, it's a great deal." I was like, "Oh, how much is it?" He's like, "Half a million." I was like, "What?" Then he showed me the file sizes one CT scan occupies. He had to buy new computers just to handle them. To your point, if you're going to get the machine, create the electronic file, then you've got to transfer the file. It's probably going to go through a new system. That's why, so most people don't realize this, that's why most hospitals have to get networked because the files they move are ridiculously huge. They can't rely on Wi-Fi. It's not a thing. It's got to be networked. It's crazy.

Cindi Carter:

You're right.

Albert Chou:

What I was saying is when you're not in it, it's hard to think of all of maybe the gaps or the things that need to work together. And so, when you're working with these teams, do they understand why they need to do this to make sure the information transfer is secured or do they come in, unfortunately, the reality is sometimes the security people, it feels like a big brother like it's kind of annoying, "Ah, I don't really want to do this. Cindi, you're telling me I got to do all this stuff?"

Cindi Carter:

I love what you just said there. Do they know why? I think that that's where we have an enormous opportunity in cybersecurity, in information technology. I think that we have an enormous opportunity to really, instead of leading with the what or the how, we need to lead with the why, because think of every five-year-old that asked the question, "Why, why? How old is your baby now?" Well, I mean-

Albert Chou:

She's eight.

Cindi Carter:

She's eight. Okay. Think about when she was five or even younger than that, and it's why, why, why. Think about kids ask that question all the time because why? They seek to understand. They don't understand the world around them yet. They don't have the experiences yet that life gives them. We need to do the same thing from a cyber and from an information technology perspective and really lead with why. Why Is this important? Help them understand the journey that that data goes on from that patient encounter, from that experience. Help them understand, obviously, they see it in the news all day long as well, but they need to understand why their particular healthcare system could be vulnerable to a certain cyberattack.

Once you help people understand they why, the what and the how becomes so much easier to implement and so much better. You have a better collaboration around how to solve the problems, because it really does take people, process and technology. I'm sure, Albert, you've heard this from all the folks that you've talked to and we actually just talked about it.

Albert Chou:

Well, people are the weakest link.

Cindi Carter:

No, no, no, no, no, no, no. I do not agree with you. I am going to go on record. I absolutely do not agree with that statement. I think that people are our greatest asset, they are our greatest strength and we have the opportunity to educate them, tell them the why, help show them the why and help give them the knowledge that they can confidently make the right decisions when they're handling that sensitive data. They are the front line, they are the absolutely people are our strength. I'm going to leave it at that.

Albert Chou:

No, that's good. That's good. I love it with a little positivity. One of the things at the top of the conversation talked about was like, hey, you personally, or whether your company or you can tell me it's a company prediction. That your company's betting this way, or you personally, you're betting this way. Tell me some of the things, because you kind of alluded to at the top that you think some things are going to change in 2023 and maybe 2024 or in the next few years, what do you think is going to change in your field over the next few years that hopefully you're... I mean, you're a positive person so that you're excited about like, "Yeah, this is going to help transform this industry"?

Cindi Carter:

I talked a lot, not only just at the event that I was just speaking at, but just in general with other chief information security officers, CIOs, CTOs, and anybody else that'll really listen. But we talk a lot about when you're creating an IT or an innovation strategy or you're creating a cybersecurity strategy, and it used to be where we had this two to three-year mid-term plan, and then you would have your long-term vision out five to seven years. Well, that five to seven years stuff, technology changes so rapidly now that those strategies, those cybersecurity strategies don't even exist yet.

We have to create a future that doesn't really quite exist. We have to protect a future that doesn't yet exist. How do we embrace that and how do we ensure that we're setting our organizations, whether it's a healthcare, financial institution, manufacturing facility and whatnot, how do we set them up for success?

One of the things that I think, and again, along with people, process and technology, one of the things that I've talked about my whole career is this concept of technical debt. You may have heard this term before, those investments that these healthcare organizations have made in equipment that's 25, 30, even 40 years old that was never intended to be connected to the internet. But guess what? Yes, they are unable to be patched, but there are compensating controls that we can put into place in order to protect them.

We think in terms of how complex our world really is, but when you think about technology and you think about those smart refrigerators or your smart thermostat or your smart cars, and we think about how much easier life is, but at the underbelly of all of that, there is an integrated system of technology, of cybersecurity helping to enable that. And so, I think when we think about the things like the technical depth, there are so many technical and cybersecurity capabilities that organizations have that they, number one, may not even have fully implemented. It may still be collecting dust on the shelf, or number two, they may have implemented it, but yet they haven't even configured it properly for their environment. Then number three, it may be implemented, but who's watching what it's doing, or it may just be sitting there outdated, unpatched, whatever.

I think as we move forward in 2023, you're going to see a lot of that complexity in IT and the cybersecurity fabric start to become simplified. Back even just five years ago when I was working in a healthcare financial institution, it was all about, well, let's get the best of breed. Let's get the best

antimalware, let's get the best firewall, let's get the best endpoint protection. You get my point. Then you end up with this boatload of cybersecurity and technology tools that the security team as well as the folks on IT have to support. There's like most organizations have more than 40 capabilities that they have to support. Think about that, 40 capabilities when you're dealing with a team of maybe one or two people. That's a recipe for becoming what's the anti-antifragile.

Albert Chou:

Just fragile.

Cindi Carter:

Yeah, that's the recipe for fragility. Yes. Thank you. My gosh. I think I need to eat lunch. My brain is starting to misfire the neurons.

Albert Chou:

You're all good.

Cindi Carter:

But that is a recipe for that. I think about my security operations team in an example like this, where we were managing more than 40 or so different security capabilities. I mean, these folks had, you said you had big screen monitors on your desk there as most people do. They had three of those 24-inch monitors stacked on top of each other. They had six total. Then each one of those monitors was subdivided into probably six different windows. Their eyes are on this all the time, trying to look at all the blinky lights or any of the yellows or the reds that are popping up. One of my team members just hit their head on the desk and went like this. I said, "What's wrong?" They said, "I can't learn any of these tools well enough to really know if it's effective."

That's when it just hit me. I said, "We need to simplify." Consolidation is something that I think is going to help us optimize our IT and security capabilities and be able to do that so that not only are the teams that are supporting them not getting burned out, but the spend is less, you're dealing with less licenses that you have to renew. Think about it when a license expires and no one knew about it and then something stops working and that takes hours and hours to figure out, "Oh wow, what just happened?" Oh, that license expired that we didn't even know about on, something that we forgot we were relying on. I mean, there's so many different examples of that. I think that consolidation and that optimization is something that is going to be at the forefront of every CISO, CMIO, CIO, CTO conversation as we head forward into 2023.

I touched a little bit about preventative medicine or preventative cybersecurity practices. Really, when you stop to think about those preventative measures, there are so many things that we have done over the last decade, even the last 20 years or so, of being able to create some really amazing things that we can do to detect and respond and help us recover from those cyberattacks. But we need to think a little further, we need to shift that mindset a little bit further left now and think about, well, what could we do to stop it to begin with? That takes that people process and technology to come together to do that.

And so, I think that that's where more and more organizations cybersecurity has a seat at the table, their voices being heard, they are part of every conversation. Security is now able to be seen as a value-add for the organization instead of this standalone group of people that sits in the corner with their hoodies on. Am I right?

Albert Chou:

Yeah. They're effectively the protectors of your business going forward. When you think about that optimization simplification, that's something that we hear continuously now that it's 2020. It's late 2022 now, this episode's probably going to release in early 2023.

Cindi Carter:

Great.

Albert Chou:

But for anyone out there listening, I think it's clearly obvious that the United States or the global economy is heading in a different direction, it's uncertain at best. There's going to be more businesses that are going to look to make investments that are cost-effective. They got to save me something, they got to save me something. When it comes to that connectivity or simplification of integration of tools, that is going to be a priority because I think you're right, CISOs are going to look at them like, "Well, it costs me so much to maintain this." You can tell me it's best to hear, A is B, A can be best, B can be best, but the cost of connect A and B sucks. I can't deal with it. They're going to want-

Cindi Carter:

No, you're right. It's not just the cost though. I want to focus on the burnout factor of the humans that are there to support all of that. When I was on that panel, the clinicians were talking about the burnout in the healthcare space. They were talking about with the pandemic, the nurses, the doctors, everyone else.

Albert Chou:

Absolutely.

Cindi Carter:

They're so overworked, underpaid, tired, trying to save lives, doing all the things in their heart and everything that they came to work to do. It's the same thing for the cybersecurity and the IT folks. We just want to make the world a safer place and we want to make sure that people live their best lives and that's how we can really work together in this space. I do think that in the sense of that consolidation, if you will, part of that does help alleviate that burnout.

Albert Chou:

Absolutely.

Cindi Carter:

We need more people in every single industry. We talked a lot about cybersecurity talent shortage. When you hear these stories, I mean, who in their right mind would want to go ahead and join a cybersecurity team if you're going to be up 24/7, 365? I mean, at the end of the day, there has to be something there. I know that every person that I share my story with, this is just where at the intersection of healthcare and IT cybersecurity is where I found my purpose. This is something that resonates with me. The number one goal of cybersecurity is human safety, page six of your CISSP. Think about that in terms of all of the other industries that are out there. The clinicians, their number one goal, of course, is the best outcome for their patients' lives, keeping them healthy, keeping them

comfortable, whatever stage that they're at. Financial sector, they want to help protect people's investments in their future and help people live their best lives, their livelihood and lives. You hear the theme here, it's our lives!

Albert Chou:

The same thing. No doubt about it. Well, Cindi, it was awesome having you on our show. Thanks for sharing-

Cindi Carter:

Thank you.

Albert Chou:

... your knowledge and expertise in an area that we don't talk about I think enough here on this show. Look forward to having more healthcare guests in 2023. I can make that prediction come true.

Cindi Carter:

Please do.

Albert Chou:

Yes, absolutely. It's something we all care very much about, and like I said, it affects our lives a great deal. I want to say thank you again for joining us on the show, but before you leave, it is time for the lightning round. The lightning round is brought to us by Salesforce platform, the number one cloud platform for digital transformation of every experience. Cindi, this is where we ask you questions outside of the world of work or sometimes it's kind of related, but anyways, it's a way for our audience to get to know you a little better. Are you ready?

Cindi Carter:

I'm ready. Go!

Albert Chou:

All right. You mentioned earlier that you're an absolute road warrior that most of your work is done in the field. How many airline miles have you logged, the most airline miles have you logged in one calendar year? From January 1 to December 31st in a year, you logged how many miles? Your biggest year.

Cindi Carter:

I don't know if I could even answer that right now. I didn't start in January of this year logging miles, because Omicron put a nice little dent in that. But since the middle of February, I can say that I've probably been on the road all of but four weeks and my status on one of the airlines that starts with a D and ends with an A is pretty good. It does help to get those little perks that make life a little more comfortable when you're traveling at 33,000 feet.

Albert Chou:

There you go. What's a travel tip you have for someone who might be about to embark on a role that puts them in the air quite a bit?

Cindi Carter:

Stay hydrated.

Albert Chou:

Stay hydrated. Cindi, thanks for again joining us on IT Visionaries. It was fun having you on as a guest. Thanks for sharing what's happening in the healthcare sector and we look forward to seeing you out there. For those interested, you can look her up. Just Google her name, Cindi Carter. You will see that she is speaking at many conferences to come and I'm sure many more will get added. If you guys want to go out, check her out, check out Check Point and check her out. Thanks again for joining us today on IT Visionaries.