Albert Chou:

This is IT Visionaries, your number one source for actual 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.

Sean Doyle:

Ultimately, when it comes to cybersecurity, we're trying to build as we go along. So you can be already in this game for 10 or 15 years, but you're always reskilling. And that's a problem, it makes it a difficult area in some ways, but it also means there's also an opportunity for people to come in. Whether you're already a professional looking to do something new, or whether you're just outta university, there's a wide number of routes. The way into cybersecurity is not just through a computing degree.

Albert Chou:

The need for effective cybersecurity has never been more pressing than in today's growing digital world. But are there enough skilled cyber workers to keep up with rising demand? On this episode, we'll discuss the extent of the cybersecurity skills gap with Jill Thomas, the director of engagement, capacity, and resilience program at the Global Cyber Alliance, and Sean Doyle, lead at the World Economic Forum's Center for Cybersecurity, hear their thoughts about what's led to the cyber worker shortage, and how a tremendously successful instructional program called the Cybersecurity Learning Hub is going to help train new leaders in the field.

Looking for more key insights from IT leaders? Our sponsor Salesforce Platform has partnered with Pulse Research to uncover the latest data security trends and best practices, find new tactics to defend against phishing, ransomware, DOS, and DDoS attacks, and more. Download the full report at salesforce.com/securitytrends.

Welcome everyone to another episode of IT Visionaries, and today we have two special guests that are transforming the way we are gonna be skilled and how we're gonna work in the future. We have Jill Thomas, she is the director of engagement for capacity and resilience at the Global Cyber Alliance, that's globalcyberalliance.org, and we have Sean Doyle. He's a lead in the Center for Cybersecurity at the World Economic Forum, wefforum.org. Sean, Jill, both of you, welcome to IT visionaries.

Gill Thomas:

Great to be here.

Sean Doyle:

Glad to be here.

Albert Chou:

Awesome. Listen, for our audience that may not know exactly what each of you do or what the organizations are striving to accomplish, let's start there. Jill, what is the Global Cyber Alliance?

Gill Thomas:

So we're actually a nonprofit organization and we were founded in 2016. We work on projects and programs that build tools that will reduce cyber risk, and we make them accessible globally. We're also

engaged in several projects that help close the cybersecurity skills gap, and hence we're also a founding partner of the Cybersecurity Learning Hub as well.

Albert Chou:

Awesome. Sean, what is the World Economic Forum?

Sean Doyle:

The World Economic Forum is also a nonprofit. It's the organization for international public-private partnership. So what we do, we bring together leaders from goverments, from private sector, from NGOs, and from academia together to try and solve some of those more tricky, difficult cross-border problems. And if you're looking at something that has deep economic and social significance, how we manage our cybersecurity is definitely among those, and h- making sure that we have people who are sufficiently skilled to do that is top, number one problem we all need to solve.

Albert Chou:

Yeah, so l- I wanna go into that in just a moment, because I wanna kinda frame up the size and scope of this problem, or this challenge, right? So when I take a look at something really simple, in how the world doesn't unify on power outlets, every country has its own power outlet, which is pretty crazy. So we already know that the world doesn't really like to standardize on things, right?

But we also agree, and I agree with you, that cybersecurity, that our world, our future t- our present depends on the internet, and our future will as well. And so this idea that there needs to be a standardization, I agree, 100%. That is ... But when I think of the task in front of you, I think of how monumental of a challenge that must be. Because like I just said, we haven't even standardized on power plugs. How are we gonna standardize on internet protocols, security protocols, skills? So many things that we would have to accomplish. Sean, I'ma start with you, because you just mentioned a little bit that skill is actually where it all begins. Talk about that. Why is that where it begins, why is that the focus? Because the task at hand is massive, right? (laughs) Why is skill where it all begins?

Sean Doyle:

So people often talk about digital transformation. What that actually means is transforming the processes, the activities, the way everything's done within an organization and a business. So when we're talking about building skills, and back to what you're saying about standardization, there's definitely, we need to set standards for minimum levels of skills for whatever it is to do with new technologies and how they're operating.

But ultimately, when it comes to cybersecurity, we're trying to build as we go along. So you can be in i- already in this game for 10 or 15 years, but you're always reskilling. And that's a problem, it makes it a difficult area in some ways, but it also means there's also an opportunity for people to come in. Whether you're already a professional looking to do something new, or whether you're just outta university, and we can go into this later, but there's a wide number of routes there. The way into cybersecurity is not just through a computing degree.

Albert Chou:

Jill, one of the things that we see is who is leading this push? Who is leading this charge for reskilling, upskilling, unifying the globe, the workers around the world on a cybersecurity standard? Do we see it more happening in the private sector or the public sector? It sounds like it's coming from the private

sector, because of the, the massive, uh, shortage of workers. I'd love to hear your opinion, where do you see this push coming from?

Gill Thomas:

I think it's across all of those sectors that you've just described. Particularly there is a huge gap in terms of cybersecurity skills i- within the, within the industry, within the private sector itself. There are so many openings for cyber professionals, so many vacancies that need filling. And particularly where we're seeing, uh, with digital transformation, the move from people related jobs to technology f- doing those functions themselves, and therefore we had the workforce, so we had those people that just want to retrain, reskill, so that they're able to support the need for those, um, technology-related jobs. They've got so many transferrable skills that are available, it's not just technology and cybersecurity, it's about people skills, it's about soft skills, it's communication. There's a whole host of areas that people move into within cyber. It's not just technical.

Sean Doyle:

Albert, if, if you look at the stats for what the gap is in cybersecurity professionals, the minimum estimate is about two million globally.

Albert Chou:

The shortage of workers to jobs, two million?

Sean Doyle:

Yeah, shortage to jobs, and if you look ahead five, six, seven years, we're looking at close to three million just in the US.

Albert Chou:

(laughs)

Sean Doyle:

And every country needs cyber skills. So wh- what that creates is this sense of, not blind panic, but I grew up in a farming area, so I think of it a bit like a horse race. The horses don't necessa- they're all going in the same place, they're not necessarily aware of all the other horses and what they're doing, but they're going hell-for-leather.

So in a small number of countries we've seen goverments are actually able to do a really very, very good job. You've got countries like Israel, which, which simply 'cause they have this, the, the system of government coming through the military, it allows them to, to train people up, um, a bit more easily. Very few countries have that kind of setup there to, to build off.

But what it means is you've got the private sector trying to fill these jobs, or trying to create the skills, often in isolation, one company against another. Just looking again at that gap, if we're to fill this it can't be a competitive space. There needs to be at a minimum, uh, coordination across sectors, uh, as to how to create the cyber skills that they need, 'cause they can be quite specific sector to sector.

And some, a lotta governments are doing excellent jobs [inaudible 00:07:58] things, everything from raising awareness just in the public discourse, to setting up training, um, as only goverments can do, thinking very, very long-term, starting training in secondary school or high school level, and looking at

how to take graduates who aren't necessarily from technical skills and bring them in to the wider area of cyber work. So who's doing it, where's the push from? It's from everywhere, it's from absolutely everywhere. The, the problem is that at the moment there isn't enough people kind of running, not even together, but even in the same direction. There- there's a degree of, "We must do something," action is being taken, but not as coherent as we would like it to be to really start filling, uh, the skills gap.

And one of the really interesting things about this, cybersecurity, traditionally people who come out of universities have got very good evidence that you can train people up in an apprentice model.

Albert Chou:

Okay.

Sean Doyle:

What that means is that this is a way that you can create skills, lifelong jobs, 'cause this problem is, is not going away, it's one that we have to manage. So the skills, lifelong jobs, for people who haven't gone through the, you know, the full end of university education system. They might've come out of high school only, they might've gone straight into the military at, at a younger age. Whatever it is, we found the, this is something that can be converted. It's just we haven't yet got to the point of scaling these apprenticeship schemes, either within a country or across sectors.

Albert Chou:

So a couple of things that both of you said that I think about right now is, the first thing is I think about one of my good buddies who's a, he's the deputy commander of JSOC, the US military, and he said, "In the history of man, there's always been somebody who wants what somebody else has." And so now, it used to be lands, now it's data, data is wh- often al- analogous to gold. So data is the new gold, and people want it. So 100%, you're absolutely right. As we b- become more reliant on the internet, there will be more nefarious actors, this will increase the demand for cybersecurity.

The other thing, Sean, you just touched on just a moment ago, which I, I wanna dive deeper into, is this idea that there has to be some type of unification system to push it forward. You mentioned Israel, and one of the things that's been cool about IT Visionaries is we've had a lotta Israeli defense companies join us on the show, and you are correct. So for those who have not heard those episodes, or aren't quite familiar, in Israel, every citizen is required to serve in the military, and a lot of this funding is coming from their country, their government. Do you see this, Sean, as something that other countries will start adopting, where, "Hey" ... Because the, the desire to learn is a major thing. The payment, or the financial aspect of how do I p- you know, how do I afford to take these courses is probably another. Do you see goverments taking a bigger role, similar to what Israel has done to pushing this forward to close that skills gap? Where they're gonna say, "Hey, we're gonna introduce programs, we gotta get more interested, technologically smart, competent people that wanna be in this field."

Sean Doyle:

Yeah, I think we're in a lucky period at the moment, at least for someone like me who's looking at this from a research perspective, in that a lot of goverments are experimenting, and they're doing quite different things in some places. So some are doing, I think in the, in the US example, they're doing an awful lot, but one of the things that's coming out is messaging. So President Biden came out a couple of months ago and said, "We need to train X million cyber people." Very quickly you have private sector companies lining up and saying, "We can do at least some of it."

So Fortinet, one of the partners in the Cybersecurity Learning Hub system which we try to use to bring people into cybersecurity, we can ta- we can talk a bit more about it later, but they made a separate statement saying they will train up one million people. So in countries like the US, the government is doing stuff, but it's also setting the, the environment for pr- the private sector to take steps.

If you look at smaller places, so, um, Dubai has a cyber capacity building program for its city, which is linking in elements of cyber skills and cyber skills development into almost e- every bit of funding it has for things such as transport, schools, development, et cetera, et cetera. So that's a very different model. Depending on the size of the country, they'll look at it differently.

What we're seeing, the good news, is lots of countries are beginning to link things up. Now, where is the big gap? It's sometimes in the countries of the Global South, where they're often trying to think, "Well, we need to develop our basic digital infrastructure, and cyber skills, it's not that they're a luxury, they're simply not something we can access." Thankfully, again, what we're seeing is countries taking a really wider view. In the last year or so, the World Bank has set up a trust fund specifically for cybersecurity skills, which it's linking to its Development Fund funding going into countries in the Global South. So the problem has yet to be solved everywhere.

Albert Chou:

Sure.

Sean Doyle:

On one, we're seeing really interesting experiments, but on the other, we're also seeing an awareness that this is, thi- this problem needs to be solved to some extent globally, or it's not gonna be solved at all, 'cause everyone's interlinked.

Albert Chou:

That makes total sense. Jill, do y- for most subjects there's like a curriculum, building blocks, "Hey, we learn this together." If everyone's attacking this problem in a different way, is there like a standardized curriculum? Like, how do people unify on that? Because different companies are gonna have different needs. I can imagine if this was left only to the private sector, let's say I had a huge s- skills gap shortage, well, I'm gonna open up training where I have gaps, not where I have strengths. And my, if my gaps and strengths don't match someone else's, now, if I were a student, let's say, to learn these things, I'd have two options. I'd basically have two options. I can learn this skill, I can learn this skill over there. I don't have a unified way to build, I guess, many people together. I'm assuming right now every- it's like every person or organization for itself, but do you see this type of merge, will it start happening, do you think? Uh, some type of curriculum standardization?

Gill Thomas:

Yeah, and again, it is across different countries. So for example, in the UK, we had the National Cybersecurity Center, they operate a scheme known as Cyber First. And that takes students, provides them with extracurricular activities from, from a young age. So puzzles, so, um, competitions, residential courses to introduce cybersecurity to these students, and then moving through to sponsorship and bursaries as they move through university.

We also support work placements and, um, we provide summer placements for some of these students so they can actually apply what they're learning in the classroom into the real world. Um, we work with other consortiums, um, those t- 12 universities, for example, form what's known as the Consortium of

Cybersecurity Clinics. And between those, there's curriculum that is being standardized, because it makes a lot of sense that you only need to develop these curriculums once, and then they're repeated across different organizations, different universities. They're then able to not only learn these skills in the classroom, but also go out within their local communities and help those small businesses within the local communities identify what those risks are in those small businesses, provide them with support and advice, and improve the, um, the cyber posture of those small businesses, whilst at the same time giving themselves those skills, in the field skills that, which will be so important as they actually move into careers themselves.

And there's a number of different examples of, of that taking place in different countries as well. You know, there's a number of different schemes and projects that are out there. We, we also work with the Atlantic Council, who developed a program, a strategy ga- challenge known as Cyber 9/12. And that brings students from a whole host of different disciplines, it's not just about computer science or cybersecurity courses, it's about bringing a diverse group of disciplines together to look at an unfolding cyber attack scenario and work out, "How would I be advising on policy? How, what recommendations would I be providing?" And giving them a real-life snippet of what life in cybersecurity is like.

And through competitions and through initiatives like these, we're actually seeing people making career choices to move into cybersecurity, whereas before they just genuinely wouldn't have had a clue as to what was involved.

Sean Doyle:

On the question of companies only looking to fill their own gaps, uh, through better experience, a lot of them are learning that that's not going to be enough. So if you have the, the huge gap in available positions, and as Jill said earlier, nobody is unemployed for long in cybersecurity. The workers are very, very mobile. And what that means is that you need to think very much about not just what's there at the moment, what will keep our staff there, but also what's coming down the line, whatever new technologies are there. And what that means is that when it comes to developing training, very often we're looking at creating a career path that gets someone into cybersecurity, and after that it's a question of following what's happening on the job. Following whatever the, the latest technical developments are out in the market and building your skills around that.

Again, it's, it's, it makes it difficult when it comes to one organization trying to solve this problem on their own. I- it does create opportunities if there's a degree of collaboration across sectors.

Albert Chou:

So that makes complete sense, and part of the reason why I have the two of you here today, because there's a new thing being developed right now, and that is the Cybersecurity Learning Hub. This is, for our audience that n- is not aware, the links are gonna be in the show notes as always. But this is an initiative led by our title sponsor, Salesforce, support from another company called Fortinet, they're gonna be on the show later on, and the Global Cyber Alliance, and the World Economic Forum.

The goal of this learning hub is to democratize access to cybersecurity skills by providing free and career-oriented modules that give people a route towards in-demand roles. This sounds pretty darn good, 'cause like, I think to myself, "I'm a dad, I got kids, they wanna know, 'What should I be doing?'" I always think to myself, "I don't really know." Uh, (laughs) 'cause I think back to when I was a kid, and most, you know, like, you've probably seen that stat, that most of the job- like, whatever percentage of jobs today didn't exist 20 years ago, I was like, "This is exactly where you are today, son." Or, m- my kid is, uh, f- he's four- he just turned 14.

Right, when he's an, an adult, the jobs that he might have access to are not gonna be the same as what's available right now. When you think of a program like the Cybersecurity Learning Hub, you know, give us a picture. How did this come about? Each of your organizations, what are you guys trying to achieve? I think we got a good picture. And then I'd love to know how we get there, because that's, that's what everyone wants to know, is like, I think, I agree with you, this has to happen. The question is how.

Gill Thomas:

Certainly. So the Cybersecurity Learning Hub was actually, um, initiated in February 2019, and we work with, with the other partners to provide content and to provide courses on that on the hub. There's now 60, o- well, over 60 courses that are available for people to use, and it really meets those users where they are. And that's really important. What we've found, we've just recently, actually, been conducting a survey, and what we find is that 23% of the people that have responded to the survey, they're a professional, they're looking to make a career change. An additional 5% of those that have actually left work and been out of work for a period of time, and are looking to get back into the workplace and are looking at cybersecurity as a career.

Nearly half of those people as well, when asked what your current knowledge, uh, of cybersecurity is, most of them suggest that they're, they're beginners, they don't really have experience. So it's really providing those users with the ability to learn and to look at, "If I were to go into cybersecurity, what kind of roles could I expect to do? And when I look at those roles, what skills do I need? What training do I need?" And from looking at that, they would then look to take on a number of those courses, career-orientated courses, to arm them with the information and with those skills that would enable them to, to get jobs in those chosen fields. Since 2019, there's been 690,000 courses that have been completed on the learning hub itself.

Albert Chou:

Can you repeat that number?

Gill Thomas:

690,000.

Albert Chou:

Okay, that's a lotta, that's a lotta time, that's a lotta hours being spent learning. (laughs)

Gill Thomas:

It is, it certainly is. And in September, there were, um, about 40,000 courses that were taken from the hub. Um, and each course actually has, on average, a 97% completion rate. So we're doing something right here. Um, it's really, real- it's a vital resource, and we're certainly very, very proud to be a part of it.

Albert Chou:

Sean, what do you see pushing that completion, 97%? I mean, I, I don't think I complete 97% of anything. Uh, I barely watch all of a Netflix movie. So this is (laughs) this shows to me, like you said, there's appetite, right? And then probably, shows to me that the, the course is probably pretty good. Like (laughs) where d- where do you see pushing it forward, and, and also, the catalog's gonna keep changing. Of course, you kinda hinted at that. Give us an idea of what you see happening. Who is contributing to the courses to make it, I guess, this good?

Sean Doyle:

So wh- why is it as sticky as it is?

Albert Chou:

Yeah.

Sean Doyle:

Once people start, they keep going. So I think that's partly the interest level of cybersecurity, it's a really broad topic. To, to give you an idea, I didn't come from a technical background. I came in from, I used to do investigations into political skullduggery and money laundering and stuff for-

Albert Chou:

(laughs)

Sean Doyle:

... for banks and private [inaudible 00:21:22]-

Albert Chou:

That's kinda cool, actually, yeah. (laughs)

Sean Doyle:

... so I mean, v- very non-technical. Yeah, it really was, it was great, great work. But, but the thing is cyber actually includes all of that. And if you're interested primarily in technicalities, cyber includes that as well, and everything in between. So once you start digging into this, the topic, it has a puzzle to suit every type of mind. That's why once you're there, people start getting hooked into it. Uh, there's always something for you. [inaudible 00:21:47], just take a look at, um, the last two months. Little country of Albania in the western Balkans has been attacked twice, its public services, by what's been attributed by many to the Iranian government. How is that known that it's the Iranians, uh, why do they come to that conclusion? Partly they look at actually how the attackers move, how they operate. I- does this look technically like i- it's an Iranian group?

But then a lot of the rest of it is this contextual work around, well, why would anyone attack this? They're not getting any money from it, et cetera. Who would be against this or that? And it turns out, I, I didn't know until these attacks came out, but that the Albanians have been taking a lot of, uh, Iranian political refugees, and giving them a, a place to speak. So there already you've got this idea of everything from technical to high politics and everything in between. And it's a really very interesting world.

So once people start learning about [inaudible 00:22:36], uh, for example, me again, don't come from a technical background. But it's the other bits that got me hooked in. And the more you start learning, the more you want to know about the technicalities, and I think vice-versa. So that's why it's quite so sticky.

Albert Chou:

So you come from a crime solving background, and I, I don't disagree at all, because the way ... It's one thing to say, "I wanna steal data," or, "I'm gonna hack your system, try to hold your system ransom for money." Of course, that is a massive fear of just about every private institution that there is. You know, if we think about the evolution of humanity, I'm not saying what's right or wrong, but the reality is lands,

kingdoms, countries, they get invaded. W- you know, there's always, like, kinda back to li- that comment I made before wh- on, at the JSOC level, there's always somebody who's not happy with what they have and wants something else. And today, how you get that is through data. You just hinted at it, Sean, like, it's done through data. So I never really put it on that spin. For, for the courses, are they all just technical? Are they, like, just like, just technical courses where people are kind of drawing conclusions to say, "Okay, if I learn this skill, I can then apply it here?" Or is it like done in a narrative fashion, Sean, like you just suggested (laughs) where it's like, you know, this is how you solve political crime? Because the way you described it is, is very compelling, you know. And I think to a, a manual that just says, you know, just bits and bytes, that's not as interesting. (laughs)

Sean Doyle:

So i- it has the lot, it has the lot. But the way it's been done is that we're, I, I think we're going to have a new release soon in the next month as well, it's looking at creating these career paths. So showing you how maybe you're really interested in technical architecture, and that's your thing-

Albert Chou:

Gotcha.

Sean Doyle:

... but not only showing you a, a way to go and do that, but showing you how it connects into something like threat intelligence, which has those technical elements, but also has the context, the what's happening in the wider world, what does this sit in type question with it. So it's providing that access to everybody.

I think, whether the overarching narrative within it that really does resonate with people once they start looking at cyber is that this is a- really about helping things. Cybersecurity, it's like nursing, it's like firefighting. You are actually keeping everything running. And going back to, you're keeping hospitals running, you're helping keep schools running. You're in those roles that are really keeping things that matter, not just because they make profit, running, while also keeping everything else, um, i- in some way, if not running, then at least being able to help companies and organizations get back up and running after a, a major attack has occurred. So it's when you put all those things together tha- that it has something that's a puzzle for everybody who likes puzzles, um, that it, it has all these various options, and that as you get into it, you get to see how useful it is to your day to day life and the world you're living in and the people you care about.

Albert Chou:

Jill, I'd love for, to hear your perspective too. What do you see happening that's making this so compelling for the audience? Because those numbers, that completion rate, the way just Sean describes the different angles and routes that people can take ... And I- and I'd also love, after you explain it, what's making this so compelling is like, how's it getting made, I guess? This is really fascinating, like h- (laughs) because I go back to that plug example I use from the start. It's really hard to get consensus. So someone is coming together (laughs) and saying, "This is a great curriculum, or we're building a curriculum in a way, with some level of consensus, that says, 'This is gonna ge- pull people through.'" 'Cause tha- that success rate, or completion rate, is a, is a, you know, is an example of that.

Gill Thomas:

And it's a, tackling the, the problem from all angles. So it's tackling the problem at the source of the problem, the internet, addressing what, um, how the internet works, and, and trying to achieve that s- standardization, and identifying those malicious domains, the, the threats that are occurring, and just stopping them hitting the internet in the first place, but at the same time then also working with those communities, all of which have got slightly different requirements, slightly different threats, and understanding those and doing something to help those users to prevent them from falling victim to a cyber attack.

Every day is, is different. The, really fast, the internet initially was developed as a communication tool by, by academics, essentially. And it was a force for good. But it's been taken over by these malicious actors, and so what we need to do is defend against that. And that's where people like, um, you know, the mi- the military, who is all about security, is taking those skills, that situational awareness, those soft skills and being adaptable, being able to retrain and being able to use new skills, and using that every single day and moving into, um, cybersecurity from, from that perspective.

If I look personally at myself, I started off years ago with a, I did a degree in electronic engineering. I moved into telecoms from a technical/sales/business development angle. I took probably six, seven years out of the industry, and when I came back, the difference, how fast technology has moved forward, what the internet is, it's a force for good, but at the same time, as I say, it's being taken over. And that just draws you in to find out more about it. What can we do to prevent that, and how can we protect those vulnerable communities as well? And that's a really, really important part.

So there's all of that aspects that it appeals to. The caring profession, the security profession, it's also, in terms of reskilling, if you're looking at moving, and we have people within Global Cyber Alliance who have come to us from nontraditional routes, should you say, it's about moving into a career and constantly learning and constantly refreshing. And it's just such a great place to be. And there's always going to be that need for people.

Albert Chou:

So give me an idea, how does, uh, and any one of you could say, h- how does like, like a skill or a course get added to it? Who does that? For example, le- let's imagine this new, uh, def- network defense protocol is created. It stops any bad traffic on your network. Okay. Well, how's it get into the course?

Sean Doyle:

Yeah, so one of the ways we do th- think about that is, what's happening now? I, I think I said it earlier, that this, this is always a movable feast. Everything is always changing and developing. You know, some of the food is falling off-

Albert Chou:

(laughs)

Sean Doyle:

... one side of the table, the waitress is coming, adding more different dishes. And the way we're, think about that, partly f- from our perspective in the Forum, we're lucky to have access to experts from just about every sector you can think of. So we recently did work on, I think, electricity grids and, and oil and gas.

Albert Chou:

Yeah.

Sean Doyle:

Really core providers of everything we do. If the electricity grids get shut down, forget about everything else. And the, the reason for that is, is that the people working in that area said, "Things have, things have changed, and w- we want to get that notion out there that things have changed."

And something like the Cybersecurity Learning Hub, the aim of it is to democratize access to cybersecurity skills, but raise awareness of, of the fact that these things are going on. So it's very easy for us to come to groups in, you name whatever's on the cutting edge at the moment, and say, "If you think people need to be aware of this, but also in a way that they're going to do something about it, here's a way in o- uh, to do that. Please start coming to us, telling us what people need to know." And we can develop some learning content off the back of that.

Albert Chou:

Oh, so there's a strong appetite to also create the materials, it sounds like?

Sean Doyle:

Absolutely. So I mean, we would see this, in the Forum, we would see this as part of a supply chain for s- building up cyber skills across countries, and the learning hub is already beginning to translate lots of its content into seven or eight languages other than English, and we've seen there is global appetite. So what this is, this is the starting point. It's to let people know this is there, it's interesting, there might be something about it that's for you, and then give the notions of where they can give afterwards.

After that, we're getting into the, the slightly tricker- trickier question of getting, um, companies and goverments to start setting up apprenticeship setups, uh, collaboration on skills a- and employment, that sort of thing. This is a starting point. And it's one of the things we do need to start solving the problem.

Albert Chou:

Jill, do you ever see this evolving? Like who, or will there ever be someone who's like, overseeing, like, some type of accreditation, certification that says, "Hey, Albert has gone through courses A through Z, this guy is pretty much qualified to do this job," do you see that coming in any near future?

Gill Thomas:

In terms of the Cybersecurity Learning Hub, we do provide the users with a, with a path to say, "These, you know, these are the courses that you need to take," and they do get certificates. In terms of accreditation, that's not specifically something that we've addressed so far within the Cybersecurity Learning Hub. There are a number of professional training organizations that are available that would be able to provide those accreditations, so it may be, um, a, a sort of globally-applicable, but also within individual countries as well. So I think that, in terms of the learning hub, that's not at this stage something that we've, that we've been considering.

Sean Doyle:

And Albert, just o- on that, si- as, as Jill said, there are a lot of very good professional certifications out there. Getting to one that's completely internationally recognized, I know there are a number of, there

are a number of goverments who are raising that up as a possibility. I'd be skeptical as to not whether that can ever happen, but to whether it'll happen in, in, in time to matter to your son who's age 14.

Albert Chou:

(laughs)

Sean Doyle:

Just because cybersecurity i- is one of those areas on which goverments continue to, uh, agree to disagree. More frequently they're breaking into, into geopolitical blocks around it, so, and you can just see that in the UN. So getting that down for goverments to agree saying, "In every country, we recognize X, Y, and Z as the best." Politically, it's problematic. I- it's also, once these things are recognized internationally, they can become a little bit frozen in time. And for something that's moving as quickly as cybersecurity, um, it may not be the worst thing that we have i- a wide range of different, uh, professional qualifications and certifications.

Albert Chou:

Well, look, I think I said it at the top of the show, this is certainly a problem worth attacking. I don't know if it'll ever get solved, but I, I agree with you both 100% that it has to happen, there has to be some type of mass effort to upskill, reskill as many people in this industry as possible. And just like my analogy to the power plug, it's probably never gonna get standardized in 100% alignment and agreement, but that doesn't mean it's not worth doing. And I agree with you 100%, getting more people interested in this field is critical and paramount to our future.

When I think about, like you said, Sean, the attacks, whether it's geopolitical or private sector attacks, this is not gonna change. This is the new way we are. Until a bigger threat comes in, effectively cybersecurity's not gonna go away. We said it from the very top of the show, there's always been someone who's not happy or wants more. Data is going to be how they take it. Therefore cybersecurity is never going away.

You're in a never-ending race. We've had CISOs on this show saying like, "Hey, the second you solve a problem, another problem emerges," and you're just constantly battling, you know what I mean? Like, you're battling the bad actors and you're trying to solve for problems. Do you ever see like the learning curve going to taper? 'Cause I think the learning curve is always gonna go up. I just don't know if it's ever gonna taper, where, "Hey, you have enough skills where i- (laughs) for wh- for a moment it looks like the bad actors can't get in front of you," or is this one of those things where every year there's gonna be more courses, there's gonna be more solutions, there's gonna be more things to learn? Like it- it's always gonna be exponentially growing?

Sean Doyle:

Human technology hasn't stood still since at least the printing press, back in the 14, 1500s. So as long as connected technology is moving, so will the threat. Now, o- on the other hand, there are sone developments that a- are very positive. We are getting better at automating some elements of cybersecurity requirements that takes out a lot of the human error in certain areas, it takes ou- out some of the works, bits of work in, in cyber that were manual and sometimes [inaudible 00:34:17] painful. But that's being done because the attacker is also adopting automated technologies, and we actually just need something that can respond at the speed of a machine.

So a- as I said, yes, things are always changing. Usually something is changing for the better, and if you're in the role of a, you know, a chief information security officer, then you can be fairly guaranteed that whatever's happening for the better, something more difficult is also around the corner as well. So people in that particular profession, they're never going to be bored. They're also never going to sleep all that much.

Albert Chou:

(laughs) Hey, you gotta keep it honest. (laughs)

Sean Doyle:

Th- th- they're interesting, interest-

Albert Chou:

I like that.

Gill Thomas:

It is that saying that says, we have to be right 100% of the time, they only have to be right once. Um, and that's what keeps you on your toes.

Albert Chou:

(laughs)

Sean Doyle:

And that's also for pos- positive developments. Organizations getting better at saying, "We will get hit. How do we recover?" Rather than just, "I want to be 100% safe," which isn't possible.

Albert Chou:

That's true, we've seen investments in, uh, CIOs come talk to us about disaster recovery. They're more concerned about disaster recovery than ever before. It used to be like, "Hey, I got this backup server, it turns on when I get hacked." (laughs) It's like, how it's like disaster and recovery's like one of the biggest things. There's more levels of encryption and layering so that if you do get hacked, like hey, it doesn't matter, you just stole a buncha garbage. There's all kinds of new emerging fields, which are all, like you said, Sean, they're all part of cybersecurity. Just d- depends on where are you in that domain? Are you in the recovery side, are you in the prevention side, the encryption side? There's many places to play in this, this field.

Gill Thomas:

Moving it into the boardroom, t- making sure that the board is taking accountability and are responsible for that response, and, and seeing cybersecurity as a real business risk now, which maybe a couple of years ago, they never did. It was just something that the IT department looked after, are responsible for, but now they're absolutely accountable and it's absolutely a business risk.

Albert Chou:

Well, Sean, Jill, it was awesome having you both on the show, kinda showing us and explaining to us what's happening in the world of cybersecurity around us, how the World Economic Forum is partnering together with different groups and organizations, and the Global Cy- Cyber Alliance are partnering together with private entities to build curriculums to help people get into the field, to upskill in the field, to reskill in the field, basically expand the field, right? (laughs) And it was really great hearing all the things that are happening in that space.

But before you go, it is time for the lightning round. The lightning round is sponsored by Salesforce Platform, the number one cloud platform for digital transformation of every experience. Sean, Jill, this is where we're gonna ask you questions outside of the world of work, so our audience can get to know you a little bit better. And we're gonna theme it a little bit towards cybersecurity. Do you bank from your phone?

Sean Doyle:

Yes.

Albert Chou:

Do you use a password manager?

Sean Doyle:

No, because [inaudible 00:36:58]-

Albert Chou:

(laughs) Do you have crazy, randomized passwords for every single account, or do you kinda use similar ones a little bit too often? (laughs)

Gill Thomas:

I have different ones.

Sean Doyle:

I'm on the too often.

Albert Chou:

(laughs)

Sean Doyle:

I am my IT security team's nightmare, as they consistently tell me. I know what I should be doing, I don't always do it. I think that's the problem for, uh, uh-

Albert Chou:

(laughs)

Sean Doyle:

... infosec professionals everywhere. Most people are like me, unfortunately.

Albert Chou:

It's like dieting. We all know vegetables and fruits are the best for us, but that doesn't mean we'll, that's what we'll eat. (laughs)

Gill Thomas:

(laughs)

Albert Chou:

Do you use IoT devices? 'Cause I will tell you, I have a dumb home. I ... But not 'cause I'm a cybersecurity person, it's 'cause I'm actually cheap. But the dumber my home gets, the more safe I feel, actually. (laughs)

Gill Thomas:

I don't really have, uh, many, I don't really use IT- IoT devices in the home, no. I don't see the need for a IoT toothbrush, for example.

Albert Chou:

(laughs)

Gill Thomas:

Auto- [inaudible 00:37:52].

Albert Chou:

How about you, Sean, are you an IoT person?

Sean Doyle:

I do have some, but I minimize it, primarily out of paranoia. But, but also it's, it's, uh, it's not always necessary. But the thing to keep in mind is whatever about what's in our house, IoT's gonna be much more necessary in things like manufacturing, factories, everything else.

Albert Chou:

That's true.

Sean Doyle:

So security of IoT is gonna be exceptionally important.

Albert Chou:

(laughs)

Gill Thomas:

And especially for those developing countries as well, Sean, in terms of how, how it supports agricultural uses in farming as well, so absolutely.

Albert Chou:

Yeah, we've had some guests from, uh, Bayer and Monsanto, and some of th- even Deere talk about some of the things that are happening in how food production is gonna be computerized, or how computers are gonna play a part in food production in the future, pretty fascinating stuff.

Sean Doyle:

And Albert, not to s- not to slow down the lightning round, but that's an actually an area of optimism. IoT security, goverments are working well together to take a lot of the, the stress away from retail users like you, me, and Jill.

Albert Chou:

(laughs) Well, listen. I always like asking this question, these questions to CISO, uh, or people in this realm, because you kinda know about the threats, and then it's, it's always interesting to see like, what about you personally? Like, what do you think? And, uh, it sounds like you guys are similar to myself. You recognize the threats, uh, you probably don't take all the precautions that you need to, but you, you do take some precautions. Uh, you have some trusted devices and stuff, and, uh, if you're like me, whether you use IoT or not, I always think to myself, when I read about these IoT hacks, I think to myself, "Man, it's actually just further supporting my cheapness." I'm just actually cheap. I don't actually c- (laughs) I'm not worried about the security. I think one of you two said, it's like, I don't really find the need to have a wifi enabled pillow. Like, it doesn't make sense to me. (laughs)

Gill Thomas:

You know, and often, with IT- IoT devices, quite often we're, we've been sort of programmed to look at, look at the cost, um, as opposed to the actual security aspects that are associated with IoT devices. So if you like to use IoT devices, it's checking out those security credentials as opposed to how much does this cost, necessarily. Because it can cost a lot more in reality, um, if it hasn't got those, those levels of security.

Albert Chou:

Well, listen, I got a fun story for you. There was, we had a woman, uh, from Darktrace on our show once, and she was talking about how one of the casinos got information hacked from a Bluetooth enabled fish filter, for all those fish tanks in the casino? It was able to connect to the network somehow and able to capture player registrations and player cards, like the high rollers? It was able to capture their data, so they could s- see their player cards, and then they could actually use the player cards, that what the people were doing was they would come in with the player card, and what they do is they're swiping it, and it gets them, like, bankrolled. So they would get bankrolled chips, they'd leave, come back and cash their chips with this nother person, and walk out of the casino with money. And this was all done because of some Bluetooth enabled fish filter. (laughs) So (laughs) that's an expensive fish filter. Sean, Jill, it was awesome having you on the show. Thanks for sharing all the things that are happening with the Cybersecurity Learning Hub.

For those that are interested, it'll be linked below. If you listen to Sean and Jill, by the time you hear this episode, there already will be more courses than there are today, so I don't even know if it's worth saying how man courses there are today. Thank you for both for joining us on IT Visionaries, it was awesome having you.

Thanks for listening to IT Visionaries. We wanna hear from you. Let us know how you like the podcast by leaving us a rating and review on Spotify, Apple Podcasts, or wherever you listen. IT Visionaries is created by the team at Mission.org and brought to you by the Salesforce platform, the world's leading low-code platform. If you love the thought leadership on this podcast, Salesforce has even more IT thoughts to chew on. Take your company to the next level with in-depth research and trends right in your inbox. Subscribe to a newsletter tailored to your role at salesforce.com/newsletter.