#244 - Breaking into Cybersecurity (with Christophe Foulon)

G Mark Hardy: [00:00:00] Hey, at some point in time in your career, you had to break into cybersecurity. you've probably moved on from that point, and you're helping to mentor others. But let's talk to somebody who has done a tremendous amount in helping people get onto their cybersecurity career tracks. Stay tuned. We're gonna cover that right now.

G Mark Hardy: Hello, and welcome to another episode of CISO Tradecraft, the podcast it provides you with the information, knowledge, and wisdom to be a more effective cybersecurity leader. My name is G Mark Hardy. I'm your host for today, and I have a special guest, Christophe Foulon, and he is also a podcast host. So with any luck, we might end up doing a dual podcast.

I think that's a first for us. I've only done what, 246 podcasts so far, so it's about time I started, co cooperating with others. But anyway, Christophe, welcome to the show.

Christophe Foulon: Thank you so much for having me. I would say, [00:01:00] your podcast has been an influence on my podcasting career as I've grown in the industry and I've followed yourself as well as Ross over the years. And, excited to be part of this podcast.

G Mark Hardy: Yeah. I'm glad to have you on board. They've heard great things about you, did a little bit of homework and found out that, as I said, you'd had your pocket. But first of all. A little from your background and and we'll go from there so everybody knows why it's worth while to listen to you.

Christophe Foulon: So grew up in the Caribbean, started tinkering with computers, eventually decided I. I'm great with tech, but I love helping businesses. I love helping people solve their technical problems. At the time, decided I didn't really want a computer science degree, so went to school, got my bachelor's in business.

Then economy went down the tank, [00:02:00] decided, Hey, if I'm gonna struggle for work, might as well do something I love and enjoy doing. Quit my job. Went, got some certifications. 'cause even back then, having certifications were one of the first things that recruiters screened for. Got some certifications, got my first help desk role, and then started to really see, wait, people are doing things.

Insecurely the easy way just to get their job done, and I found myself coaching, helping, mentoring the business into doing things more securely as part of my help desk role and found out of. This whole new industry focused on cybersecurity. Took me seven years to eventually transition from help desk into cyber, but got there and that's when I wanted to start to [00:03:00] give back and help others who wanted to do that, transition them themselves.

That's when I created the podcast with my co-host, Renee Small. that's when we started. Collecting the knowledge for some of the books that I wrote. How to develop your cyber security career path at any level. How to hack the cybersecurity interview. all with multiple co-authors because in my perspective, we need a diverse perspective in how to do this.

None of our paths were unique. None of our paths were straight and narrow. there's multiple ways to get there and we can use hints, tips, and tricks from everyone and implement them in our approach with our own passions, with our own things that drive us so that we have our own fulfilling career.

G Mark Hardy: that's a good point. So you went from [00:04:00] health desk, which is it plugged in? Is it turned on to unplug it and turn it off? I'm meant security now. We don't want that going that way, so we go the opposite direction. But more importantly, like a lot of us in cybersecurity, we started out somewhere. And usually was in technology.

It doesn't always have to be, it could be GRC, it could be compliance and other areas like that. But there's an allure, there's an attraction to it. And for those of us who have landed here and find it fulfilling, one of the things that I think is great for everybody is that it's not a static type of a profession.

you learn something and that you might be a master of everything today. Six months from now, things are changing. we've got Windows 10 is going off the grid pretty soon, although it looks like Microsoft has said, Hey, we'll give you double secret probation for a year, but then you want another year, it doubles, and another year it doubles again.

And then you're gonna order two to the 10th power if you wanna stick around for 10 more years. I think the Navy did that with Windows XP. [00:05:00] Microsoft said, yeah, we'll just do it if you double every year, the support contract, and somebody who was bad at math on the government side, now this is anecdotal, so I might be wrong, said, okay, fine.

All of a sudden they're paying 1024 times as much on their contract in year 10, but it's a good lesson learned that. Technology moves along with or without us. So you've written a couple books and you talked about it developing, your cybersecurity career path and how to break into cybersecurity at any level.

And I think that came out about four years ago. and Gary Hayslip, who's been on our call, and you and of course your, partner Renee, were the author of that and then hack the cybersecurity interview. I kinda like that name. and you did that with, Ken Underhill and Tia Hopkins, whom I've not had on a show, but for people who are.

Listening to our program, usually they're into cybersecurity. Usually they're up at a ways they're trying to, either they are CSOs maintaining their skill sets at this level, or they're hoping to break into that level of the, boardroom or workroom, if you [00:06:00] will, or at least a corner office or maybe an office with a view, or at least something that doesn't end up being in the third basement. as we. As you had worked with people, getting them into their careers, what did you find were some of the biggest challenges that people face when they said perhaps like yourself? I like the idea of cybersecurity, but I'm not in cybersecurity and I, gotta get there somehow.

Christophe Foulon: first let's look at the allure. There's the allure of the CISO title and there's the allure of the CISO paycheck. You don't understand the requirements of the continuous learning, the burnout, the long hours, the on call, the incident response, the being the potentially sole neck to choke should something happen.

[00:07:00] All of these implications of that title. Because they're not as broadly discussed. And so a lot of people say, oh, I wanna become a CISO when I grow up. And then you have maybe the more. Senior individuals going, eh, I don't know if I want to be a CISO anymore. it was nice. I learned my lesson, but, someone else can do it now, or I'm fine with being a director.

I like to create the strategic program to implement the strategic program. I don't necessarily need the title and, the burnout, the extra hours, that aspect of it, unless there's some true level of shared responsibility between you and the stakeholders of the business where you're discussing who really owns the risk, and whether you're [00:08:00] advising them as to.

Where they take the risks and you're really listening to you how to take the risk, and they become an effective partner in these risk decisions versus going, oh, it's a CISO's responsibility for everything because cyber was somehow related in there.

G Mark Hardy: Yeah, so what we find then is, as you had indicated, there may be some allure. it needs to be more than, if you will, the money or the title, because that's gonna be very unsatisfying doing a job that you don't like. You find stressful, which is going to be, we'll, just be quite honest about that. it is gonna have long hours, not every day, but when, something hits the fan, you're the person on point and you've gotta be there and make everything come in.

And quite honestly, these days, we, a lot of us are worried about being the Chief Incident Scapegoat [00:09:00] Officer, when we have seen issues like with, Tim Brown, whom I am going to be hopefully doing a podcast with him next week, and we'll talk a little bit more about his experiences. but in general, we look at it and we go, do you really wanna be there with a little red dot following you around from the board with respect to your accountability?

And the answer might be that we're okay. from my military career, I had served in command nine different times. I went back and looked through some old records. I found out the selection rate for command was a single digit percentage back when I was up for commands. And so if you got one, you were.

Unique. If you got two, you're one in a hundred. If you got nine, then you're a, singularity. but that said, that didn't lend itself to putting on stars, for example, because there's a career inflection point, and this is one of the things that we wanna make sure that people understand.

I've said this many times over many shows, is that your technical skills do not beget [00:10:00] management skills. Management skills do not beget leadership skills. And leadership skills do not beget political skills, and quite honestly, I was politically, not competent. I will just be very brutally honest about that.

And to a certain extent, no matter how great you are as a leader, your people will follow you anywhere. They'll be there 72 hours nonstop working around the clock because they absolutely, you've motivated them to be on the point, but yet somehow you might find yourself. Sitting there just below the glass ceiling wondering what's happening because you spend all your time with your people and spend all the time with the right executives who could influence your career path up.

And so at what point in time do you think that somebody who's entered a cybersecurity career really starts the need to develop this political awareness and savvy? Or could they just simply say, I just don't want to go there from here. I'll be very happy. Being a director at some point, I'll be very happy retiring [00:11:00] at that point.

I don't really wanna play with the C level thoughts on

Christophe Foulon: I, I, would say it, it's up to that individual. it's where they feel that. They're emotionally rewarded with their career. Some people don't like the politics. Some people don't like the dealing with the board, they don't like dealing with, This department's fighting with this department and you become the mediator.

they don't like those conversations. They rather focus on the technical component or they rather focus on creating, those business solutions or creating that security architecture to deal with, the bleeding and edge technology and how we can solve those use cases. And we need all those different types.

Of characters within an [00:12:00] organization for it to be successful. And you might wear more than one of those hats, but as a senior leader in the organization, you need to blend. Many of those hats together, and you could be technical, but if you don't have the political or emotional intelligence to work at the board level to work with your other executive leaders in fighting for budget, fighting for headcount, fighting for who owns the risk and the remediation and those sorts of activities, then you'll end up being the one.

Burnt out 'cause it all gets shoved on your plate.

G Mark Hardy: That's a good insight. And so what we find out is that in some careers, as a military officer, at least it was from mine, it was up or out, and the idea was as you either progress to the next level or they, said, Sianara. thank you very much for [00:13:00] playing. have a nice life. We're gonna keep everybody else moving.

And it wasn't because that there wasn't room for you at that level, but there was always a constant replenishment going on. And so what we found out then is at certain points in certain careers, yes you can plateau and stay there. If we look at something like a Microsoft or an IBM, they have fellows, they have brilliant technical people.

Some of these people are Nobel Prizes. They've got PhDs. They're not leaders. They don't want to be leaders. They probably couldn't manage their way out of a paper bag, but yet they contribute brilliant technical insights that the managers, the leaders, the political, folks turn into revenue, turn into products, turn into jobs for others, and things such as that.

So it's actually, it's a virtuous ecosystem. You're not being exploited here. And when I've come up with stuff, and for example, I got. My name on my first patent recently, and everybody's you worry about that. I said, I don't really care about, assigning that patent out to a company or something like that.

'cause there's no way that I can build the [00:14:00] infrastructure to go ahead and maximize that value. And I didn't invent it to make money. I invented it because it was a tough, problem that needed to be solved. And I figured it out and they said, that's pretty cool. Or Nobody else has figured this one out before.

Off we go. So what we find then is that for people who. Get into cybersecurity. And this is an interesting question for you here. 'cause based upon your books and things like that, you say how to break into cybersecurity at any level. A lot of us think you gotta start at the beginning. You enlist as a, an E one, and then you work your way up through the ranks.

But in cybersecurity, can you say, Hey, I wanna be a director, or I wanna start out as a CISO, or is that unrealistic? And if it's not unrealistic. What are the pre-quals that make somebody able to laterally move into our career at a higher level?

Christophe Foulon: So there's all types of different CISOs and, yourself as well as Ross, have covered this in, the past, the different [00:15:00] archetypes, the builders, the breakers, the union, the, rebuilders,

the solutioner. So you can have someone that say. Comes from GRC, that comes from IT, that comes from the business side that understands the risk that the business is taking or the bus, the direction that the business is going and.

Understands that perspective. And then they have the leadership below them to advise them on the technicals, on, Hey, these are the technical risk concerns, these are the legal risk concerns. And if they heed that advice in a meaningful way, they can still be an effective CISO. if they take that into consideration.

Not everyone looks well on [00:16:00] that, and if they become the scapegoat officer, the community of course goes, oh, they were in music or they were in liberal arts. That has nothing to do with their qualifications. Their qualifications are more. Do they and understand the complexities of the business requirements, the legal implications, the legal requirements, the and the other risks that the business is taking at the time.

Do they have the right advisory, internal or external to make? The right decisions. And then are they able to influence the business leaders at the table, at the board to get the right funding and the right decisions for the risks that they're looking to tackle at that time? And that's really where all the. Everything [00:17:00] comes to center. And where a good CISO is built less than where they got their education 30 years ago, what certifications they might have got 20 years ago or what they're studying today because you, can't study every single thing that's happening. one example in the pre-call we talked about a new innovation or a reuse of an innovation for a Microsoft technology to embed it for a different use case. And I didn't know about it six months ago and you didn't know about it now, but we can share this knowledge with each other, overlap, our competencies and advise each other as a community on how we can tackle this together.

G Mark Hardy: So what we have then is an interesting model. I'm sketching it out here as we talk, [00:18:00] as a, to be effective as a chief information security officer, it is not necessary that you came up through the ranks as we. Determine, and we see that in, in the real world. But it is helpful to have credibility with your people.

And so it doesn't mean ignore the technology, but it doesn't mean you're not gonna be asked to sit down their hands on keyboard and then reprogram something that way. It is essential that you be credible with your leadership in the board and the organization that you speak the language of risk, that you speak the language of the organization, most likely business unless you're in government.

And that is non-negotiable. And as you just pointed out. Okay, I may not have a technical background. I need to have some technical credibility, ideally with my team so that A, that I can earn some respect. But B, they don't pull a wool over my eyes. But if you pointed out the very important value of having a network of peers, a network of other places of people who have had a chance to explore and learn different areas so that I'm not just Google searching, how [00:19:00] do I do something?

Or today, everybody just looking at their AI engine. Hoping it's not hallucinating on you when it gives you an answer, but having some genuine conversations back and forth with people who have done the background. I was not a lawyer, but I can talk to friends who are lawyers and gain some insight in some of the legal implications.

I was not in GRC. I do have my CISA, my auditor ticket, and I got that. Wow. You talk about years ago in 2001. So it's been a long time, since I've had that ticket. I remember when I got to Ernst and Young, when I went to work there, they said, don't tell anybody you got that, or that's all you're gonna be doing is these dumb audits you wanna go do in the fun cybersecurity stuff.

But what if I like audits? then, of course, to each their own. So now what we see then is that when you come into the cybersecurity career path. Your focus really needs to be up. If you're gonna be operating effectively at a CISO, it does then call into question what happens if you come into a position where you don't [00:20:00] have a well running organization?

We're not always gonna step in when everything is running perfectly. Everybody's highly motivated. You've got the world's best qualifications Met has offered them a hundred million dollars each, and they all said no because they wanna stay and work for you. How do we deal with that when we're now in a CISO role?

We start out and we realize things aren't working the way they should be, but I don't have the technical chops to go fix them. Any insights in terms of how somebody could proceed?

Christophe Foulon: This is where your people leadership skills need to come in. 'cause you need to understand. What are their personal motivations? Maybe they're in the wrong role. Maybe they're in a security role when they prefer to be in an infrastructure role. Maybe you have folks on the infrastructure team that have more interest in being on the security team.

Maybe you can cross match your resources and have shared [00:21:00] responsibility. Between the teams or have a fusion between the teams so that you can blend those experiences and start like that. oftentimes new leaders when they come in, they'll have an assessment from an external organization where they can point out weaknesses, where they can point out best practices.

That could be one approach. I know another leader that loves to start from the people aspect and do personality assessments to see what are the personal drivers for all of the members on their team. Figure out those drivers and then work on those drivers to drive. The team building the comradery and the personal motivations behind his team first, then build the skills and competencies where he see he or [00:22:00] she sees gaps in the team to build those up.

And then if they do have additional budget to recruit in or grow up from the organization.

G Mark Hardy: I think it's an excellent point because in a certain way you're acting as a coach, and if you were to come in as a coach of, let's take an example, American football team and the team's doing poorly, and you realize. Person you have playing quarterback is one heck of a kicker. And the person that you have as a wide receiver is an amazing, tackler linebacker, and all of a sudden you realize you've got the right people.

They're just in the wrong spot. So that's part of, assessing that. And since you'd come from the, help desk world, originally you'd appreciate this at a friend of mine many years ago that I knew up in, in the Baltimore area and Toby was in charge of the team and he had read up about. The Myers-Briggs and the 16 different profiles that could be done, and he did those inventories.

For those who aren't familiar with Myers-Briggs, you look at four different axes [00:23:00] of personality preferences. It was, initially used in World War II to try to help the US Army put the right people into the right type of a job because they're trying to place millions of, people at that point. And what he found out then is that much like the.

Football analogy where people in the wrong position, people were not in the areas that they enjoyed the most. They were doing one thing, but they hated it and just grounded out because, it was a paycheck, but when he put them in areas where they. Aligned with their preferences, the productivity of the team, sort morale went up, things got done and he didn't change his people.

He didn't change the payroll. And so that's an important idea. Have you seen other tools other than something like a Myers-Briggs Personality Inventory, the MBTI that have been helpful for CISOs or other people in that position to reorganize their

Christophe Foulon: by name, but just, by more so having informal conversations. For example, if you have [00:24:00] someone that doesn't like to be meticulous and detail oriented and following the tracks, they might not be a good SOC analyst. They might not be a good forensic analyst. They might be a good help desk person because they can, talk to the user, find out what was happening, gather.

All the details and then escalate it to the right team. but they wouldn't be the one kind of following all the breadcrumbs to exactly what the error was in the memory stack. so there's the informal way and then there's a structured way and I think cost, of the organization, maturity of the organization, all those considerations are part of it.

Even the. Mentality of the leader and the mentality of the team. I know some [00:25:00] folks see these personality assessments as fufu. doing these as informal assessments, conversational, one-on-ones. By just asking them these types of questions to gather what their personal motives are or where they feel that they gain the most power or where they wanna grow their career.

and just doing your own table analysis of if you have the right players in the right place, could, be a low cost, low code way of doing it.

G Mark Hardy: Yeah, and you can also look up, someone like Daniel Kahneman, who passed away a couple years ago, I think at the age of 90. but as a young psychologist, he was there with the, early days of the Israeli army and they had a very. Touch and go process of getting the right people in the right jobs.

They weren't doing very well and he said, Hey, let's make it methodical. Let's do this. And they all fight thought, and [00:26:00] you're gonna turn us into automatons. But he said, no, this is a process. Stick to it. Ask this question, this. Take a little bit of time. Reflect on it. Then come up with a decision and their decision process went way up.

it's interesting that as a psychologist end up getting a Nobel Prize in economics, because you take a look at why we are predictably irrational and why we have, thinking Fast and Slow was his book. And Ariel, I think did the, predictably irrational book. But there's a lot of different things we can make ourselves available that are outside of the CISO bookshelf.

these are not all cybersecurity books. A portion of them are, but a lot of 'em are that interesting thing. The other thing to keep in mind also is that cybersecurity, for whatever reason, tends to attract and hopefully retain neurodiverse people. And so what we find out is that when we're kids and didn't understand that, people would just get labeled, okay, this guy's just weird, or a nerd, or whatever.

And then we realize that in certain cases, in the cybersecurity world, that [00:27:00] natural tendency becomes a superpower. Somebody who could focus on 20 different things simultaneously. Track them all, like an air traffic controller, do extraordinarily well or turn off the whole world. Focus on just this one thing and drill in.

Drill in and stay focused until you say, Hey Christophe, when's the last time you went to the bathroom? And you go no, I guess I gotta go. And so those, which in a traditional world, people look at you as scan and go, yeah. We find out. Particularly in leadership roles that we can empower people to do extraordinary things if we can align them with those unique characteristics that they have.

And what historically people would argue would be a limitation or even a, workplace handicap, becomes a superpower. You as the leader, not only can increase the productivity of your team and the results you get, but you're gonna help the morale of everybody else. 'cause people are doing what [00:28:00] they wanna do and you're doing some good for your people.

And so I think that's one of the rewarding things you get in the cybersecurity.

Christophe Foulon: Absolutely and that's why I used a coaching moniker, as part of my own personal brand. And I do a lot, I did a lot of self education courses on coaching and mentoring to understand the psychology there, to bring that out to help facilitate and mentor and strategically develop relationships, conversations, ideas from a diverse set of individuals. Within a group, within a new team, within a new client, because as, a CISO, you have to do that. And like you mentioned within the cybersecurity community, this neurodiverse [00:29:00] population, not all of 'em might be comfortable speaking. Outwardly to unfamiliar people. They, might be very introverted until you touch on that one subject that they're very passionate about, and then they'll explode and talk to you all night and you're like, whoa.

They're not introverted. They're, totally extroverted. No, they're introverted because talking. To the general public in general doesn't provide them emotional power. It's very emotionally draining for them. Now talk to them about cybersecurity and say static code analysis, and they could probably talk your ear off because that is, an area that provides them that emotional charge to keep going. So finding what those are. Creates that [00:30:00] superpower within your team and allows you to take someone that might have been, looked at as a recluse or introvert, and you can turn them into an amazing public speaker because you're focusing on sharing knowledge that they know, knowledge that dear comfortable talking about.

Maybe some practice maybe. Some repetition on how to deliver, how to interact, and they can get really good at that. It would not probably be something that they would be the first to raise their hand for, but it could be something that you can bring out in them and use as an asset for your organization.

G Mark Hardy: That's an excellent point, and I have always. I've shared many times. The advice I got when I first got to, to Booz Allen was, speak every chance you get. And I had found out that many years of speaking did a couple things. One is you become [00:31:00] much more comfortable on the platform. Number two, you know how to deliver, how to have impact and how to get that and also from the perspective of we were talking about jobs and things like that, people said like, how do you get paid to speak? I said, do it for free for 20 years. It's a long apprenticeship. It's not easy necessarily. Some people say, I want to crack in. I wanna make a fortune. maybe you can at some point in time, but don't focus that initially.

Do what you need to do is get out there, master a technique, have a personality, don't be. Try to be a poor version of somebody else, be the best version of yourself. But another thing just before we wrap up on neurodiversity is the question I have with regard to the HR department is that in cybersecurity we may have a special appreciation and even a need for people who fit that, but when you go into a traditional HR department, they may.

Fail a whole bunch of the gatekeeper functions to say, Nope, this person didn't pass well on this test. They didn't do well on this interview. They didn't show up here on [00:32:00] time when they were supposed whatever. How do we go ahead and help shepherd our best candidates that we understand? Can not only add value to the organization, but will have a great personal fulfillment past the static defenses, which are not set up to allow them to be necessarily successful in getting to that day one on the job.

Christophe Foulon: let's talk about those static defenses. So those static defenses were developed for compliance reasons to make it fair, but in the end, don't make it fair because if you don't parse your resume in the right way, if you don't. State your experience in the right way. If you as a minority, whether mentally or from a different sort of [00:33:00] background, stated in the right way.

The parsing mechanisms used by HRIS systems end up excluding you from the application pool Almost. Immediately. And that has been discussed and discussed and we're almost getting to the state where we're, telling leaders, okay, for those niche population sets, if you do the same thing you've always done, you're gonna get the same results you've always done.

So change. Your approach go to smaller conferences like BSides or, women in Cybersecurity or, smaller conferences that attract that type of diverse population that have those. Superpowers that you're looking [00:34:00] for and have a informal interview with these candidates. And if you find that diamond and or rough, tell your HR, Hey.

I found someone, I'm going to put them through. You can, screen them, you can do all the traditional background checks you want, but I'm putting this candidate through, as part of the next stage interview. As a leader, that should be a capability that you have, and still be able to satisfy all the compliance requirements that you're validating.

I think the other concern that HRIS systems are facing is with the scaling of AI and AI tools to both scale applications by applicants, by hyper [00:35:00] tuning resumes, now you're getting a thousand applicants in an hour and the. I'd say the poor folks in HR that were already overwhelmed with 500 candidates over the span of two weeks now are totally overloaded and have to shut down the application in an even shorter period of time.

But you have an even smaller set of really qualified candidates in your talent pool that you have to try to weed through again. which goes back to as much as a. There's been a growth in diversity, equity and inclusion initiatives, and then we saw a swing back. Organizations need to find this happy balance of how to blend in, [00:36:00] finding what's right for them, not because it's politically right, not because there's some requirement set by the government.

Some compliance requirement that they need to set, but because they're finding the right resource to satisfy the job needs and the job requirements for their organization.

G Mark Hardy: Very good insight. So let's go ahead on the other end of a career track and say at some point in time we've gained experience, we've worked with CISO, we've maybe, held down a number of jobs, but at some point there might be a desire to say, Hey, I wanna be a V CISO or a fractional CISO, either independently by just hanging out your own shingle or by.

Aligning yourself with some other group that provides that service. If someone's gonna make that leap into the virtual or fractional CISO world, what words of [00:37:00] advice would you offer them to think carefully before they do

Christophe Foulon: Stay true to your passion. Back to what keeps your emotional. Battery charged. You don't want to do something that drains you. 'cause at this point you're maybe retired or semi-retired, and you're either doing this for fun to maybe provide a secondary or tertiary income stream. So you don't want this to lead to detrimental health effects, emotional health effects.

So you want to choose an area that. You're comfortable in that makes you happy and that you can really show your clients that you're an expert in or sufficiently qualified in to provide them with that external advisory support [00:38:00] in there. Now, this gets into the legal. Accountability responsibility, components of it.

as a virtual CISO or as a fractional CISO, when you engage with a client, you have to set a clear scope of engagement, what your client. Who's responsible for the risk? Who owns the risk, and what's the scope of services that you're providing? Are you providing advisory services? Are you providing technical implementation services?

Are you providing scoped project services? Really putting that into paper and a legally binding contract. And then just to protect yourself, have some sort [00:39:00] of cyber insurance, some sort of indemnity protection for yourself. A, you're walking into an environment where you might not know if there is a previous information exposure event that might come back and haunt you.

You don't know what. The other individuals in the organization may or may not be doing while you're a fractional CISO there, so you want to protect yourself as well. so you wanna have these sorts of indemnity insurance to protect yourself, in the event of something like that.

G Mark Hardy: And really insurance. For those of us who grew up in the risk world, we understand we're simply assigning risk in exchange for some fixed premium amount. if a company that is insuring you will take on the variable risk that may pay out, nothing may pay more than your premium, but [00:40:00] ideally. We always have to remember that those are priced in a way where they're designed to make a profit, and that's nothing wrong with that.

And reality is it's a little bit like taking the time to put on a seatbelt. You never wanna need that seatbelt. You never want it to have to save your life because even if you've put a seatbelt on for 50 years and you've never had it. Hold you back from anything. It doesn't mean you're gonna stop wearing it saying, Hey, you know it.

That's the 10000th time I've put on a seatbelt and nothing's happened. So who needs seat belts? reality is it's there, to mitigate the impact of some risky event that might be a low probability, but very high impact kinda we call the black swan, so to thing finances.

Christophe Foulon: if you, look at, say a, small to medium information exposure event of sensitive information like social security number, and then now you have to reach out to [00:41:00] a 100,000 to 200,000 people. This is considered small to medium breach. You have to reach out to them via the US Postal Service.

You have to provide them with a year of credit monitoring. You have to do a forensic analysis of the event all of this adds up really quickly

G Mark Hardy: Oh yeah.

Christophe Foulon: More than likely will surpass $50,000 really easily. your insurance premium, even for an individual fractional CISO, will not likely get to that level.

protecting yourself. The organization, on the other hand, their cyber insurance should cover their portion of this. You as a fractional CISO, it's co, it's covering any errors and emissions. That you might have done in your advisory or your implementation of the solution that [00:42:00] you provided to them.

G Mark Hardy: You had mentioning the postal service, and here's my kind of sheet of my favorite stamps. These are. Women Cryptologists of World War ii, they came out four years ago, and of course they're forever stamp, so they, hold their value. But I always like putting that on a letter because they're like, yeah, that's from G Mark.

He figured he'd find something to do with cryptography and women, things like that. So anyway, as we wrap up here, any last thoughts as you could give to our viewers/listeners? Plus also, how do we find out more information about you? Where's your podcast? And what do they say? Hey, this Christophe guy is really great.

I wanna follow up with him. How do people get in touch with you?

Christophe Foulon: so advice. Think strategically, whether it be your career, your cybersecurity program that you're looking to develop, find a medium to long timelines. So three to five years that you wanna plan some growth on, and then break that down into smaller timelines. and anything longer, anything [00:43:00] shorter.

There's too many variables in there that are beyond your control. For the podcast, it's breaking into cybersecurity. It's on YouTube, it's on Apple Podcasts, it's on Spotify, for my books. They're on Amazon. under my author profile, Christophe Foulon. And if you want more information about me, you can find me at christophefoulon.com

G Mark Hardy: Which I have up right now, Excellent. Christophe, thank you very much for taking the time to be on our podcast and if it worked out well, I'll also be on yours if we, if this becomes a breaking into cybersecurity episode. But for our listeners and our watchers out there, thank you for being part of our CISO Tradecraft audience.

We do this for you and hopefully if we are meeting your requirements and your needs help other people find us. By giving us either a thumbs up or a five star, some other feedback into the system. So they'll prioritize how CISO Tradecraft will show up in other people's feed so that we can go ahead and reach them in their career as well.[00:44:00]

I will be at hacker summer camp. That will be, I guess the week that this show comes out. So hopefully if you're in Las Vegas and you're listening to the show, come look me up. You can find me and I'll look forward to you. I'll be where at my CISO Tradecraft stuff. Meanwhile, in the time that you have available, if you're traveling out to Vegas, or even if you're not.

Make sure you stay safe out there and don't forget to help other people in their careers. It's one of the best things that we can do as leaders in the cybersecurity profession. Christophe, thank you very much and until next time, take care everybody.

Christophe Foulon: Thank you so much.