uberknowledge

Magda Chelly, CISO On Demand and CyberFeminist

The Rise of the CyberFeminist

Magda Chelly, CISO on demand and CyberFeminist talks:

Ashwin Krishnan: [00:00:02] Welcome to another episode of the UberKnowledge podcast. With me today I have Dr. Magda Chelly who can introduce herself, but it's going to take a little bit because of her illustrious career. Dr. Chelly, all yours before we get started.

Magda Chelly: [00:00:18] Hello Ashwin, and thank you very much for inviting me to be on this podcast. I'm very, very happy to be online here, and thank you for the amazing information about my career — not that long yet! Let me give you a quick overview of what I'm doing. So, I am based in Singapore, and I've been working here with my own company for around three years. I'm doing mainly cybersecurity advisory as a CISO on demand or a CISO implementer, and I built a new start-up with my co-founder, called Secucial or Security is crucial, which is an identity wallet. So, currently my main expertise, since I am in Singapore, is only cybersecurity. From my background, I'm a telecommunications engineer with a Master's and PhD in the same field and then evolved into IT security and business roles. This actually gave me different insights, not only about technology

but about the roles in IT and inside of a security-specific thing. So, this is a very quick overview. To add to it, I'm from Poland originally, and it's amazing, here we are in November in Singapore and it's like 27C degrees. Can you believe that?

Ashwin Krishnan: [00:01:39] You're making me feel jealous right now. So, one thing that I wanted to spend a minute or two on — because this is something very near and dear to UberKnowledge's heart — is the focus on women in cybersecurity as a focus area to bridge the cyber skills gap. We are very much focused on getting people like yourself and other accomplished women on the podcast. Can you talk briefly about what this means to you and why you started this?

Magda Chelly: [00:02:12] Definitely and absolutely, this is a topic that I consider very important, and I am passionate about driving it. Every time I get the opportunity to address it through TV or radio or a podcast, I do. And I try to make one very important point here: we need, together, to change the situation and that's what actually the cyber-feminist movement is about. The situation that we are trying to change is the current lack — actually the small amount — of diversity in the cybersecurity space. In particular that applies to women, where they number only 11 percent and over several years that percentage has not changed. So the story is, one day I just was searching for some keywords or something that would really describe the movement that I'm trying to build around that diversity factor, and I wrote on LinkedIn under the title CyberFeminist. From there it became a movement.

Ashwin Krishnan: [00:03:22] Wow. OK. I should remember that, cyberfeminist. It actually puts it in perspective, so thanks for sharing that. Turning your attention, and I'm actually quoting from an article that you wrote, which I found really topical and interesting, for the benefit of the listeners I'm quickly going to read it out and then have you comment on that, "A CISO or CSO should not only have effective leadership skills, but be accountable for the organization's reputation, the uninterrupted services and operations, availability of the infrastructure, and the protection of the assets — including the physical ones." Wow, so suddenly in

this one sentence you have elevated the nature of a CISO or CSO to something much bigger than I had even imagined. Can you talk briefly about why this is so, and what you have seen CISOs who are not embracing this much more expansive role end up becoming?

Magda Chelly: [00:04:24] I would say the first perception, and maybe the traditional view, of the CISO in previous years was mainly related to an IT security role, which currently has changed. And as we have seen as well, there is a lot of encouragement to make sure that the CISO reports to the board. That means that the CISO role is not just focused on technology any more, it's focused on technology or security that is enabling business. That said you need to have the same language as your board in order to be understood, if not, you do not have a place in the boardroom. I would say my main aspect here and what I really try to communicate every time I discuss this topic with senior information security managers aiming to become CISOs is that, for example, my business experience helps me a lot to achieve and be present as a CISO on demand. Why? Because I have the technological background and then I have the business talk.

[00:05:35] It's really important to have a wider view of the cyber risk for the business, how to present and how to understand the view of someone who owns a business as well as a view of someone who sees weaknesses and vulnerabilities and CVEs are different and literally not something that a business owner will focus on or even understand.

Ashwin Krishnan: [00:05:59] Now you bring up a really important point, given your technical background, the business background, and the CISO's point of view, you have an unfair advantage of naturally talking this course. How does a traditional CISO — when I say a traditional CISO, I mean somebody who's come up the ranks with a strong technical and security background and, like you said, looks primarily at CVEs and runs Pentest inside the organizations — really understand what marketing uptime really means? If I can't get my qualified leads, my sales are actually going to get impacted. So, for a CISO who doesn't have the experience from the business side, how does he or she embrace this

new world where they must be able to talk the language of the lines of businesses otherwise their role gets marginalized?

Magda Chelly: [00:06:54] I would say there are several ways to do it. One would be to mirror someone like, let's say, "A day in the life of ..." I would really suggest that because it changes perspectives and it's all about that in order to communicate the same language and understand how the other person is seeing the world, which includes the business world. So that is one option. The second one would definitely be to try, especially for someone with a very technical background and career, to listen a little bit more to news about business stocks or to business debates and understand what the priorities of the business owners are because the priorities are not the same. There is a huge gap between understanding, "OK, I will address that cyber risk because the loss regarding that cyber risk is very important for me and can damage not only my reputation, but my forecasts," versus "I need to address that cyber risk because someone told me that there is a new vulnerability up, and I need to update all my Windows servers." They literally need to understand that, especially when it comes to professionals from a solely technical career.

[00:08:18] The second point, again, listen for more business discussions and debates. Try to have discussions with business owners and understand their point of view and how they prioritize their own decisions. That is a second option that I advise information security officers. The third one would be, try to see and discover some start-ups, be part of some incubators as events. There are so many events around startups about new technologies, and this makes security professionals very clearly realize how much security is underestimated in such an environment. When we're talking about startups, their understanding or integration of security is very minimal. Why? Because they are trying to build a minimum-viable product, so they are trying to go to the market as soon as possible. Again, the priorities are not the same. The shift is really important, and we need to find a balance between the business owners or the business stakeholders and the information security professionals both coming from two

different worlds and trying to communicate with, most of the time, no efficient communication or actual results.

Ashwin Krishnan: [00:09:44] Yeah, and I think the first part you mentioned is the first time I've heard somebody talk about it in those words — just a day or week in the life of a fellow employee or colleague. Just go and see what their day looks like, so you can you can empathize more with where they are coming from.

[00:10:04] Switching gears a little bit to the vendor side, you briefly mentioned start-ups, so let's talk about the cyber washing as it relates to cloud. Every self-respecting vendor, large or small, needs to talk the cloud language regardless of whether their solution does anything meaningful for the cloud or not.

[00:10:27] In this challenging world where a CISO, like you mentioned, has to not only understand lines of businesses, but also stay relevant and be able to talk the business impact language and not just security-specific lingo, what happens when you add cloud to the mix? From a CISO's perspective, clearly the ability to even understand the nuances of the cloud, let alone the speed with which the infrastructure developers — whether it's AWS or Google or Azure, doesn't matter — I mean, there is a feeling of inadequacy that if you don't spend enough hours in a day or week to keep up with what's the latest and greatest out there, from a security perspective, you're going to be behind. So, from your perspective, given your expertise of going in and helping enterprises through this journey, what do you recommend for a CISO? How do they assess what cloud security means and what options they have at the point of deployment, but also how do they keep up with the changing landscape without falling behind?

Magda Chelly: [00:11:45] I would say the first step or important point here for any CISO out there, especially for the new ones, is to make sure that they don't assume that others or other professionals in the cybersecurity space or in IT are actually knowledgeable around the shared-responsibility model. They've been working with companies deploying cloud for certain customers and from small,

medium to big enterprises. The mistake is very common every time: they do not consider cybersecurity as part of the first design and first requirements whenever they migrate to the cloud. The basic shared-responsibility model, which actually was present for many years, is not something that we can assume that people know. As much as we want the situation to be different, it's not the case. So anyone who is looking into new technologies, deployment of cloud, must take that in consideration and make a big and important effort to make sure that the awareness is there within the team and the right stakeholders on a vote. Every time I tried to make awareness sessions, even with the IT department, I realized that they assume very often that the cloud service provider will take the responsibility of the security, which is wrong because most of the time this is not the case, unless you have a managed service which completely changes the contract. But there is another factor that is important for the company to understand, which is that other development parts of the product also need to take into consideration cybersecurity from the requirement point. And here they have developers, they have been with them their whole career developing several applications, that does not imply that they have been trained and that they have the knowledge around secure code practices. So those are the basic, I would say, steps for a CISO to understand and especially not to think that someone or the other departments have a certain background in cybersecurity. Always try to bring the right baseline and foundation from a clean, best practices approach from the point of view of cybersecurity.

[00:14:32] Can we keep up with all the technologies that are rising every day? No, we cannot. Definitely. And I like the word that I use pretty often, which is technami, tsunami of technologies. It's actually some researchers who found this word and it's amazing because it's going even more into a very complex, interconnected ecosystem with over 300 billion connected devices by 2030 and that's only an estimation. So again, we are not able to really know every single technology, understand its weaknesses and how it works. What we can do is we can have the right team working for us, with the right SMEs that can help us address those technologies. Then with the right mindset and awareness around how important the cybersecurity is and making sure that it is part of the design

and the requirement from the beginning, then we are building a healthy enterprise ecosystem, and we are building the right foundation. It's extremely costly, and it's extremely complex to make sure that we correct mistakes from 10 years ago, especially when it comes to MNCs or Fortune 500 companies. They find themselves with, let's say, thousands of web applications with no security-by-design or no-privacy-by-design, and it costs them millions to fix those problems. So, having the right mindset, security- and privacy-by-design, no assumption about the knowledge of others around cybersecurity, and always bringing the right experts to help the team understand the different technologies that you're putting in place.

Ashwin Krishnan: [00:16:28] That's a great segue into the follow-on question: let's assume you're a CISO who's suddenly been assigned a certain budget to make sure that your IaaS initiative in public cloud, pick your favorite one, is secured. And you have your existing pool of talent within the organization, which is not cloud-savvy. But then, let's say you've been working with vendor A, B and C for your network security, endpoint security, and application security for on-prem and all of them claim, "Hey, we can take you to the cloud because we have a virtual version of what we have on-prem in the cloud," or "We just acquired this brand-new start-up and therefore now we can offer end-to-end security." So what is your recommendation, not only if you are the person with the budget, but in your consultancy role when you go into an organization, what's ... you mentioned SMEs, and you can't build SME expertise for cloud overnight, so are you seeing enterprises turn to their trusted on-prem security partners first? Do they go to a big-name consultancy, which obviously a lot of organizations can't afford? Do they come to people like you with the on-demand expertise? What are the general operations that you have typically seen enterprises go through?

Magda Chelly: [00:18:00] Typically what I have seen, at least here in Asia and Singapore in particular, and I'm talking about medium-sized enterprises regulated by the MAS, which is the Monetary Authority of Singapore, and multinational enterprises with headquarters in Singapore. I have seen the cloud migration addressed in a way that they were launched — I was actually part of

some of those projects around request for proposal — and then they actually expect the cloud service provider to come back with a certain approach and a proposal helping them to assess the situation and chose the cloud and migrate. What happens here is most of the time the security is not integrated within the RFP. That means that the cloud service provider, of course, will come back, answer the questions, and will not take into consideration the security part. All the projects that I have been involved in — actually there was one in particular I was involved at the beginning of the RFE which very quickly advised on security, but it wasn't actually implemented — but all the other times I was asked to come and fix the situation after the fact. Of course, that means the choices around not only cybersecurity, but even around, let's say, data sovereignty — some of countries in Asia require it, like Vietnam recently launched a new cybersecurity law that requires the data to be stored in Vietnam — are not a consideration at all. So, it starts from a very bad understanding of the requirements related to security and privacy. This visibility of own data and applications, making sure that you have the right approach and the right requirements listed for your RFE before you go and start choosing your service provider.

Ashwin Krishnan: [00:20:13] And I can imagine how difficult that is under a time crunch, right. "Hey, we're going to the cloud, we need to be more efficient, so if security is not ready, we're going to go forward anyway." Let's switch gears, I know we have about five or six minutes left. I want to get to something that you probably have a much deeper interest and knowledge in: identity. One thing about identity that struck me, I was watching a very interesting video a couple of days ago by a lady called Bianca, and she was talking about identity evolving from just your typical active directory-based permissions to one which includes permissions and context. And it was interesting to see the context could be based on where the user has been and where they're coming from, which location etc. Other attributes that will decide whether he or she is granted access to a particular data store. So, what do you see as the evolving definition of identity in this world? Like you mentioned hyper-connected devices or over

provisioned admins because you have fewer and fewer people. Is the evolution of identity something that is top of mind, if not, should it be?

Magda Chelly: [00:21:33] It's a very interesting question, and I really thank you for bringing this topic up. My second startup is actually around identity, as I mentioned, and I believe first of all that we're going, in the next few years, away from the centralized processing of credentials or personal data. That means that the control would go back to the user. But coming back to your point in that particular article, why we're talking about contextual data in order to allow authentication for the user is because currently the traditional ways of authentication are not sufficient. I'm not bringing the right security for the users as well as for the companies. What does it mean? It means most of the time we do not have the gap between digital identity and physical identity. That means someone steals my laptop or my phone, maybe they can access my identity. Or, you know, someone just hacks my password at the end.

[00:22:42] A lot of companies do not even have two-factor authentication enabled, which is just hygiene and does not even mean that you are 100 percent secure because that does not exist. It's also a very bad misconception from the business thinking, ",OK if we do this then we will be 100 percent secure," and they do the same concerning the database of identities that they store in a centralized database, thinking that they will be enabling additional security in order to protect their database. Today, with such a complex legislation landscape across the world, with security that is going into more and more complex solutions because of the level of technology that we have deployed in our businesses, and with the number of connected devices in the next few years, we are not able to sustain the same way and the same centralized approach; we need to change. And that means that we are changing into maybe the centralization, I believe into that, but at the same time not a traditional conjugation method anymore. And I don't want to go to the details about the contextual data because it's part of my new startup, so I'm keeping that as a scoop for my next article.

Ashwin Krishnan: [00:24:09] That's fair enough. I think it's great that you are also endorsing the fact that the traditional single-data store and let's protect the keys, let's protect the kingdom, and let's store the key somewhere and we should be safe, is a myth. So, I have to finish off on this thing. You mentioned decentralized, which automatically, if I do a google search, I'm going to get to blockchain. Any final thoughts on blockchain as an underlying infrastructure, if you will, for this decentralized identity?

Magda Chelly: [00:24:47] Yes, but this thought would definitely not be related to just the security professionals, but to all of the audience to try to spread the message: Blockchain does not equal security.

Ashwin Krishnan: [00:25:01] Ok. That should be the topic of your next article, blockchain does not equal security.

Magda Chelly: [00:25:06] Exactly! I've been hearing this way too many times.

Ashwin Krishnan: [00:25:14] On that note I think we will end this podcast; it's been a really interesting conversation. Given the number of topics we have touched on pretty briefly, I'd say I'm pretty sure I'm going to invite you again for a follow up on one of these many topics. Thank you for your time, Doctor Magda Chelly.

Magda Chelly: [00:25:35] Thank you very much. And talk soon. Bye bye. Bye.