The Deloitte On Cloud Podcast

Host, Gary Arora, Chief Architect for Cloud and AI Solutions, Deloitte Consulting LLP

Title: **Cybersecurity's future: PJ Hamlen and Julie Bernard on how Generative AI helps defend against new threats**

Description: In this episode, Gary Arora talks with Deloitte's Julie Bernard and AWS's PJ Hamlen about the future of cybersecurity, including the role of Generative AI and the coming impact of quantum computing. They cover leading practices for cloud security, AI's potential to detect and defend against new threats, and why a culture of collective responsibility is essential. Julie and PJ also share their views on evolving risks and how leaders can prepare for a dynamic, unpredictable future.

Duration: **00:26:26**

Gary Arora:
Hey, everyone. Welcome back to the On Cloud podcast where we dive deep into all things technology. I'm Gary Arora, your new co-host and chief architect for cloud and AI solutions over at Deloitte. We've got a great episode for you with two amazing guests who know a thing or two about cybersecurity. Joining us are Julie Bernard, a principal in Deloitte's cyber practice and PJ Hamlen, leader at the Global Partner Security initiative at AWS. Julie, PJ, welcome to the show! It's great to have you both here. Let's dive right in. PJ, why don't you kick things off by telling us a bit about your background and the work you're doing at AWS?

PJ Hamlen:
Sure. Thank you for having me, Gary! I am the leader of the Global Partner Security Initiative at AWS and this initiative is part of a growth initiative program, where we are engaged with the world's top global systems integrators, including the top global system integrator for cybersecurity, Deloitte. A couple of years ago, we began working with Deloitte as a lighthouse partner on this program where we co-invest to develop and bring to market advanced GenAI-enabled cybersecurity offerings for our enterprise customers. Prior to joining AWS, a little over two years ago, I spent just under 20 years at the IBM Corporation, starting in professional services as a consultant and moving into some internal transformation roles, and I spent my last few years there in our banking and financial markets unit, where we began to learn more about the importance of cyber security and compliance as parts of the IBM Emerging Cloud Unit at the time. It's a real privilege for me to be able to work with Julie on a day-to-day basis and I'm happy to be here. Thank you!

Gary Arora:
It's a pleasure, PJ and Julie, we'd love to hear about your journey in cybersecurity with Deloitte and your engagement with PJ.

Julie Bernard:
My journey in cybersecurity precedes my time at Deloitte, but like PJ, I spent quite a bit of time prior to joining Deloitte in financial services, technology and operations. I've been at this consulting thing for 30 years. And I joined Deloitte at about nine years ago, partly because we are the number one cyber program and delivery team in the world. We have the size and scale to answer pretty much any question. What I really love about our time working with AWS on ConvergeSECURITY is to be able to add some global consistency to delivering a handful of our security offerings. So, we have kind of best people and best tech that we can offer to the marketplace.

Gary Arora:
That's awesome. And speaking of technology, let me start with the buzzword of 2024 and maybe in 2023 for that matter, it's the AI, the GenAI. And, so, Julie, let me start with you. With the advancements that we are seeing in AI and GenAI technologies, are these cybersecurity threats advancing and evolving as well? And with the current controls and tools that are in place with these organizations, are we equipped to handle these new threats?

Julie Bernard: We take those in two parts, Gary. So, let's talk about the threat environment to start and then we'll talk about how we all respond to them. And PJ, I would invite you to also share some of your anecdotal experiences too as you go to the marketplace on the response. But we've always had a bit of an arm race with what I'll call the miscreants out there in terms of the threat environment. What AI has allowed the miscreants to do is to go faster. So, now, we have both of volume and velocity hitting our defense teams like we haven't had before. There's also an ability to get even more clever at the weakest link, which are the humans that are sitting behind the machines, in terms of whether it's an e-mail of some sort that looks more and more real, like it's coming from their boss, or perhaps a text message.

So, you're out of band and maybe out of thinking and you're busy trying to think fast and not necessarily think smart. So, there's a couple of things there that are really advancing very rapidly. On the control front, are the organizations equipped? Well, we are bringing AI to the cyber equation, which is helping with the volume and velocity issue. That allows us to put those poor precious people that we have to really look at the veracity. So, like, is the threat real? Is that how do we tell that the issue is certain if you will, and then the variability, net new things that might be coming in, new techniques, new tactics that are hitting the security operations center in particular.

Gary Arora:
Right now, that's an insightful point, Julie. PJ, let me come to you. How is AWS looking at this challenge and the additional strategies you recommend for these organizations facing these risks?

PJ Hamlen:
So, in terms of what we're seeing from a GenAI-specific perspective, I think everything that Julie described with regard to, I love the term miscreants, she's the first I've heard use it but I admit I've adopted it, the miscreants have had the opportunity to leverage GenAI in ways that allowed essentially new people to enter the threat landscape. So, I saw one statistic that said that the week that ChatGPT was released, distributed denial of service attacks quintupled in the following days because it enabled people without prior or technical knowledge to adopt these sorts of actions to do them, and that works against us, but it also works for us in the way that we are integrating Generative AI solutions into our cybersecurity capabilities, both to address the gaps that we see in skills availability as well as our ability to mitigate or remediate cybersecurity attacks in a more rapid fashion with the aid of GenAI.

Gary Arora: So, with these new threats and the evolution that you're seeing, are you seeing that translate into a different kind of buying pattern or demands from your enterprise customers regarding security capabilities?

PJ Hamlen:
Well, I certainly will say that all of our customers in general are on the GenAI bandwagon. Everyone is very interested in the potential of Generative AI, and the challenge is actually what to do with it, and in some cases it's the hope of applying it in a situation where you don't need it. In many cases, simple machine learning will work just fine. But the impact of GenAI in isolation, in terms of buying patterns, isn't quite as significant as what we are seeing broadly from our customers and how they are becoming more mature in the way they see their cybersecurity solutions.

Our customers more recently are looking for more holistic end-to-end offerings, many of our CISOs have 40, and I've seen numbers up to 70 or more, individual tools that they use. In many cases it's best of breed where they use them for fit for purpose. The number of tools that they have in their suites are almost unmanageable. And, so, they are looking for providers such as Deloitte to come in and help them integrate those into a holistic end-to-end offering, but with choice.

They may wish to work with a particular ISV that has certain functionality, or a SIM that they want to integrate and we want to be able to offer them those choices. Another big trend that we're seeing, and this is much more recent, is they are prioritizing and asking for industry-domain expertise. So, we need to be able to provide them with industry-relevant functionality for their cybersecurity and compliance offerings, and we need to be able to bring to bear both advisory services around those and the proof that we are capable of operating in their unique industry specific environments.

Gary Arora:
So, Julie, PJ just mentioned some of the trends he's noticing from an AWS perspective. I want to ask you this: We talk a lot about organizations that have done this well, successfully adapted their cybersecurity strategies, good for them, but given your exposure to the market, can you talk about companies that have struggled or failed to respond effectively to these new cybersecurity threats that are stemming from the emerging technologies and what critical missteps or insights should the listeners be cautious to avoid?

Julie Bernard: I hesitate to make this only a security problem, Gary because I feel I would condemn the victim for best efforts in that sense. So, let's look at the security landscape or the IT landscape a bit more broadly and talk a little bit about why the job is hard. We have some basics that still we have trouble getting right. I can't tell you how many of my clients still struggle with IT asset management, end of life systems.

Other, I would call IT hygiene issues, patch management, the boring stuff, if you will. We love to talk about AI and GenAI and one of the things I love working with PJ and ConvergeSECURITYas I get to actually think about innovation as opposed to compliance. But there's still so much work to be done on the compliance front.

That makes it that much more difficult to get ahead. I also see, and PJ alluded it to it earlier, that there's so much interest in this shiny, pretty thing that is AI, and particularly GenAI, that we forget that, or particularly, enterprise customers are on piles and piles of data. It is not all neatly rationalized. It is not all neatly well governed, so you can trust the data that's on that you're going to use for your language model, whether it's a large language model or a smaller language model, however you want to think about it, and I know you spend a lot of time talking about AI in the marketplace.

So, I'm not going to educate you on that one, but understanding like what you're actually relying on as an underpinning. When it comes to the security front, we still see plenty of silos. You'll have a data protection team or an identity management team or security operations team; the lists go on where they trip up themselves is still living in those silos and not creating their own data lake in which to find the less-findable in their environment.

Gary Arora:
So, building on the strategic risk that Julie mentioned, PJ, what are you seeing in the marketplace from AWS's perspective?

PJ Hamlen:
I think Julie's perspective on this was spot on, from an AWS, particularly a cloud perspective it is singularly one thing with regard to security and the most common mistake that we see is not making security a critical element of cloud migrations from the ground up. Security should be job zero when considering whether to migrate to the cloud, and the classic mistake that we see is it is not an upfront consideration, and it is actually a major cause of why cloud migrations either fail or are significantly stalled early on, because security becomes a secondary consideration.

And then any work that has been done in that cloud migration needs to go back and essentially needs to be revisited and essentially have security built into that or have that migration brought up to spec in terms of security best practices. So, if there is any advice that I can offer for companies looking for lessons learned around not adopting best practices, is ensure that security is a first and foremost element of the cloud migration that you are making.

Gary Arora:
I feel that message should really be printed on a poster and be on every wall of every organization.

PJ Hamlen:
It absolutely should be. We need to marketize it.

Julie Bernard:
I think we have a slide on that PJ that says security is job zero.

PJ Hamlen:
I think we do have that.

Julie Bernard:
We have that.

Gary Arora:
Both your roles involve looking at the horizon and predicting the future to a certain degree, that's just the business you are in. So, for technology executives aiming to strengthen their organization's cybersecurity posture, what's one actionable step they can start implementing immediately to stay ahead of these evolving threats?

PJ Hamlen:
If I can be so bold as to say it's not just technology executives, it's boards of directors, it is business leaders in general and of course technology executives. I think what a lot of people forget is that cybersecurity isn't necessarily about technology. There is a critical human element to this and the way that business leaders can begin to get ahead of this is to just have an elementary understanding of what the threats to their business are and beginning to instill a culture of security overall.

This is really a human problem. Human error accounts for over half of all the root causes of security breaches. So, if there is anything that we recommend first and foremost, it's really about human behavior and adopting a culture of a security mindset and creating awareness to help prevent breaches or exposures that may occur.

Julie Bernard:
That's certainly the fast dollar PJ, like I agree with you on that comment. I was just thinking about my commentary earlier was about IT hygiene and a lot of this conversation has been about Generative AI. So, if you think about IT hygiene is the past and Generative AI is today, we have another onslaught coming with the discussions around what does post-quantum encryption look like or what does quantum computing look like and how does it impact the size and scale of the matter we are talking about.

So, let's just say there's a company mid-journey to cloud and dealing with all of the governance and human GUI type issues you were talking about PJ, it's like we also have to start getting ready for the quantum future. I would say there are some basics you can start with right away. Everything from like the board down governance, but then just starting to get your lists right. Where are all your encryption keys?

Where are all the connections you may have in and out of the institution to provide products and services to your end customers. I mean some of these basics sound rather mundane, but it's in the mundane that we get tripped off all so often.

PJ Hamlen:
Absolutely. I would say organizations outside of the kind of cultural element that I think I was pointing to, first and foremost conduct a comprehensive security audit to understand where your vulnerabilities are and to help you prioritize where we need to focus to ensure resiliency. Absolutely agree. I also agree with you on post-quantum. I think if GenAI is now, quantum computing is the future, and it will fundamentally disrupt the cybersecurity industry. So, it's both scary, but really exciting because there will be so much potential for that, and it is not too early to begin thinking about the implications of a post-quantum world.

Gary Arora:
And PJ, you hit a point earlier that's so near and dear to me that is in most organizations you have a CISO that's the chief information security officer, and in some ways, it gives you this false illusion that security is someone else's problem being managed by a different group and a different team, and you over on this side of the house don't have to worry about it. But that results in so much churn and becomes a hindrance in the process of product development in innovation. So, first, Julie, let me ask you this, have you noticed this kind of challenge in your engagements and what are some ways to get ahead of it?

Julie Bernard:
Well, I love some of the innovation that we are starting to see emerge, particularly as we think about how do we enable developers and development team. So, can we use solutions to help build security in from the start. We have talked about shift left in terms of building security requirements in but how do we even use AI or Generative AI to build some of those security controls into code at the start to make the lift on the back end easier and to help propel the innovation that everyone is striving for.

One of the other kinds of non-tech things that I get really energized about is the youth that's coming up. When I started my technology career, I coded in COBOL on a mainframe. I didn't have a laptop until I was two or three years into my career. We now have universities and colleges that will teach people to code and have cyber programs. The energy enthusiasm of youth is really exciting and energizing to me because they will solve the problems that my generation haven't been able to solve.

Gary Arora:
Absolutely. And PJ, anything to add here?

PJ Hamlen:
I particularly agree on the power of youth, I love it, Julie because we at AWS, we have begun to work more and more with universities to help develop cybersecurity capabilities. I think I mentioned earlier that there is a very a significant skills gap in our space, it will only continue to get worse as the world becomes more complex and we see more and more organizations migrating to the cloud. I find it very exciting that we can actually help individuals establish a career path as they emerge from university with the skill sets that they will need to make it to make an impact.

I wanted to go back to your comment about the CISO role and it has historically and from the conversations that I have with them, it has been a bit of a lonely role. There's really no one pats you on the back and says good job for the 100 days in a row that you didn't have a cyber security incident or 1,000 days in a row, but eventually something is going to happen to you and that's when you get the most attention.

So, I kind of go back to that notion of building a culture around security and making it everyone's job can and kind of take the loneliness out of that and also help that resiliency posture of an entire organization.

Gary Arora: All right. Finally, I would love to hear from both of you what emerging trends or innovations in cybersecurity give you the most optimism for the future? What are some of the things organizations can do to leverage these advancements effectively?

PJ Hamlen:
So, we keep talking about GenAI and I do want to say the excitement around artificial intelligence is absolutely warranted but what we should realize is that we are actually in the Bronze Age of GenAI, I mean we are just beginning to understand what the potential is. So, we shouldn't rush to adopt GenAI for the sake of it, but I think we all have a responsibility in our industry its potential and to think innovatively as Julie mentioned earlier about what it can do for cyber resiliency, for the good of our customers, and for society at large.

Certainly, I believe that excitement around GenAI is warranted, and personally I am excited to see where it goes. I think we both mentioned earlier and I will let Julie comment on this a little bit more what the post-quantum world will look like and while quantum computing and the implications of a post-quantum world that has to be very terrifying to the CISOs across the world. I actually think we should be really excited about it.

It it's coming, and it represents a paradigm shift in our computing capabilities and the problems that we will be able to solve both for business and for society and like GenAI I believe that quantum will be used by the miscreants, but also to the benefit of our cybersecurity colleagues.

Gary Arora:
Julie, please bring us home with what excites you the most about cybersecurity.

Julie Bernard:
Well, besides working with my friend PJ and all of our clients and customers out in the marketplace, I want to go back to AI and some things that I have said in the past and think about. I can't really call it a post-AI world because we are in it, the current AI world and go back to the human piece for a minute, there's a book called *Thinking Fast and Slow* I think Daniel Kahneman wrote it. and In the world of AI, the thinking fast part is what the machines will start taking over. The thinking slow part is where the actual intelligence that other AI is really going to come into play.

As I said earlier, when we started this, the volume and velocity of some of these threats coming in will be handled by the thinking fast pieces that we can, whether it's through quantum computing or AI address, where we are going to really need the humans to help is on the other pieces, the veracity and the variability and the things that are coming at us. I think we are sort of at that precipice of change and that's really exciting to me because it's again yanking security out of the world of technology and putting it back into humans.

PJ Hamlen:
Plus one on Thinking Fast and Slow. Amazing, love it.

Gary Arora:
I was just going to say that's one of my favorite books as well, very insightful. So, thank you for plugging that in. Awesome. That's it for today's episode of the On Cloud podcast. A big thank you to our guest Julie Bernard and PJ Hamlen for sharing their insights. If you enjoyed our discussion, make sure you subscribe and leave us a review. You can also check out our past episodes wherever you listen to your favorite podcast and you can always connect with us on social media. Thank you for listening to the On Cloud podcast. Until next time, I am Gary Arora.

Operator:
This podcast is produced by Deloitte. The views and opinions expressed by podcast speakers and guests are solely their own and do not reflect the opinions of Deloitte. This podcast provides general information only and is not intended to constitute advice or services of any kind. For additional information about Deloitte, go to Deloitte.com/about.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

Visit the On Cloud library
www.deloitte.com/us/cloud-podcast