CYBERSECURITY & AI: ARE YOU RISK-READY?

WALK IN THE CLOUD

AUDIO TRANSCRIPT

Host: Ellen Bencard

Speakers: Jacky Fox, Accenture, Managing Director, European Security Lead

Jacky Fox Bio: Jacky leads Accenture's Security practice in Europe and Ireland. With 20 + years' experience in the industry, Jacky also serves as Vice-chair on the board of Cyberireland and has lectured on Cyber Security in UCD. Jacky considers herself an active researcher and really enjoys public speaking. Jacky was awarded security champion of the year 2018 in Ireland, and was also lucky to be recognised in the EMEA SC 50 women of influence in cyber in 2023.

Intro: Walk in the Cloud.

Ellen: Cybersecurity not so long ago, it was the domain of nerds in basements, bedrooms, and IT departments. These days, as almost everything in our lives has gone digital, it's the stuff of boardrooms, national infrastructure and common sense. What are the latest trends? That's what we're exploring on today's Walk in the Cloud.

I'm your host, Ellen Bencard and I'm joined today by Jacky Fox, who leads security for Accenture across Europe, Middle East and Africa for Accenture. Though today we're going to stay focused on the UK welcome Jacky.

Jacky: Thank you very much for having me, I'm really happy to be here to talk to you today about cybersecurity.

Ellen: Excellent. We're going to start with the big picture. Security is a very long running area of discussion. What do you think has changed in the past year or so that's worthy of note?

Jacky: A couple of things. I think a lot of boardrooms have really woken up to their responsibility, in relation to keeping their businesses resilient. A lot of businesses, unfortunately, have had fairly severe cyber attacks or if they haven't, they might have somebody that might sit on another board where they know of it or their peers are talking about it. Also, we're seeing a lot of regulations and laws dictating that businesses need to take responsibility for their resilience, particularly if they're around critical national infrastructure, if they're providing power or water or something like that that they need to keep the lights on and the water flowing, and they need to be responsible in as far as they can to protect themselves from attack and also if they do have an inevitable attack, how are they going to operate while they're recovering from that? I think it's definitely come out from IT and it's gone up a few levels in an organisation and people are looking at it with a strong risk lens as well, rather than just as an IT problem they're looking at it as a business risk.

And I suppose the other thing that's very noteworthy in cybersecurity at the moment is, that it's very closely aligned with diplomatic and political issues that we're seeing across the world today. So, cyber security is now the 5th domain of warfare, and even if your organisation is not involved in warfare, you could be third party to a supplier to somebody that is. Or you could just have the same type of technical infrastructure that somebody, who is a target for somebody has and you can get literally caught in the crossfire or your infrastructure is going to have the same vulnerability, so if that's spreading around the world, you can just get caught up in that through no fault of your own. They are two things that I think are quite big. It's up more in the boardroom and the political landscape we're working in today has meant that it's a bigger risk for organisations.

Ellen: That is surely a lot more complex than the old days of just worrying about whether or not my network was secure. Let me throw another thing in there. Everybody's talking about AI this year. Does AI factor in either the protection or the attack side of security?

Jacky: There's three perspectives that I would think about from security and AI. The two perspectives you mentioned that people are concerned that if AI is used in the offensive that it will be man against machine and machine might be more powerful or faster in their response. People are worried about what happens if my team are attacked by AI? Then there's also the thought, if we're going to get attacked by AI, we better be able to defend ourselves with AI. But I think myself, the defensive stance on AI at the moment is a very supportive stance. People are using it, even if they don't feel they're being attacked by AI. They are using it to help analysts get the right information in front of them while they're trying to make a decision and even have some suggested reasons that something might be happening to help speed up the process. So, we're seeing more so the defensive side, people are really beginning to utilise it where they can for efficiency and helping getting our security analysts to be dealing with the meat of the problem and not maybe with gathering the information to analyse. But, very interesting as well, is so many organisations are looking at AI from an innovation perspective. Many organisations would say, they don't want to be left behind. They recognise that this is a whole new type of literacy that an organisation needs to have and if they're going to be using AI for innovation within their own business structure, they need to do that securely. And the types of things that can trip people up there are maybe they could inadvertently breach information out with the prompt when they're actually querying into an LLM. Also, we know that AI can kind of be prone to hallucinations and making up references, so fully and utterly believing and trusting in all situations the information that comes back to you, what you're doing, can be a bit of an issue. But also, there's a huge ethical question that we need to ask as well around what happens if a model gets poisoned, and we've seen it already, where it becomes racist or is making poor decisions or recommending poor decisions to you. How are you making sure that you're on top of that from a security perspective? And that you're able to prove and demonstrate that your decisions have been fair and based on maybe something that you don't understand, an algorithm that isn't actually an algorithm that's several pieces of information that maybe can't be backtracked and might give a different answer tomorrow. There's a whole lot of things around there that need to be explored a bit deeper.

Ellen: And if you think about the UK executives that you've been talking to, what would you say the state of awareness is? Are most senior executives clued into this or is there a way to go?

Jacky: We are getting asked the question a lot, so I would say most executives are very aware that this is going to be impactful on their business. Are they clued into the risks of it? Which would be the area that I'm interested in. Maybe not as clued in as they might be, but I would like to think that in this space we're going to learn from the past and maybe not repeat some of the mistakes of it. I would love to see people really embedding security and in the beginning of them using AI rather than only doing it after something bad has happened to

them. I do think there's a lot of meaningful conversations going on in this space. I'm talking to a lot of senior executives and board members in this space in the UK who are asking the right questions, which is positive. It's a good start.

Ellen: Yeah, that is good news. Now another thing that I think is a feature of Europe, is that we tend to have tighter data protection and privacy laws than the rest of the world, certainly tighter than the states. For example, the UK's new data protection and Digital Information Act. Everybody is trying to figure out what to do with that. How do you think that changes the landscape for security professionals working in the UK?

Jacky: I think it's very interesting the UK specifically, as opposed to Europe because obviously the UK are in and out of some of the regulations that other people are or are not and they have different flavours of them and they're going at different speeds. So, I think if you're in the UK and you're doing international trade, which a lot of people are, you need to be very aware of where your next-door neighbours are at as well as where. You're at, so that's quite impactful. Because as the world is becoming more and more global, we need to be internationally aware of data privacy regulations and looking at where you are and are not transferring information to within that reason and also because of some of the geopolitical instability that we have at the moment. We would see a lot of clients who are getting very interested in the sovereignty of their data; where is it actually being stored and getting more sensitive to that than they might have been before? Where has it been stored? Where has it been processed from? And are the right permissions in place for that to happen, or just saying actually we don't want that to happen, we want our information processed within our own sovereign data where if there's a dispute, it'll be our legal system and our jurisdiction that's going to hear that dispute. We are seeing people getting more aware of that, and particularly in public services, health organisations; they're getting very focused on where is my data being stored. But actually, industry in general like cloud service providers and technology providers are responding to that by coming up with services where they're actually geofencing and offering the optionality there that people can actually look after their data like that. Which is good. When all this started becoming a focus seven or eight years ago now, at this stage, I know it's been going on for like 30 years, but it actually became a very targeted focus about seven or eight years ago now - those facilities were not there for people to utilise, whereas today they are.

Ellen: Yeah. Well, again, good news that it just feels like everything is developing to a far more positive place than it has been. A multi part question. How are security professionals facing being part of national infrastructure and what can the organisations behind them do to help them?

Jacky: OK, from a European perspective, we have the network and Information System directive and in the UK there is the network Information Systems Regulation, which is very similar but slightly different focuses. The UK was still part of the general kind of European landscape when that started, but by the time it was being enacted they had separated so they had a slightly different focus. At the end of the day, I think what a lot of people's focus is, is what do we need to have in place in order to keep what we consider as critical infrastructures operating and that could be food delivery, transportation, media, cloud services, water, electricity, gas, all those sorts of things. And so most organisations that are providing a service like that, let's say for example electricity, they will have their own corporate infrastructure, which is maybe measuring and minding what's going on and making sure the billing and they're buying the right things in and out and moving around, which is what's making the business tick. But they also would have generation, distribution and things of that power around the place, and it's probably getting a lot more complex now because like with smart grids and also people producing power, you know from wind and solar panels and maybe bringing that

back into the grid it's all getting quite complicated actually - like what's being protected today, critical national infrastructure in that space is actually very different than what's going to be protected tomorrow. There are two key things there. One is the corporate land like that we've been working on and the other is the operational technology that is actually providing the service of the organisation. And we would see the kind of corporate dynamics in organisations like that, they're just as good as anybody else's corporate network. On the operational technology side, they generally started the journey a little bit later and probably have a little bit further to go to kind of get that in line with where we in the cyber industry would like to see it to be and that's where those regulations came in to help drive that and to get people to kind of minimum baseline standards so that they could prove and show their resilience if they get hit by something. So again. There's a lot moved in that space, but I think it's probably more to be done in that space than there is in the corporate world.

Ellen: And overall, what I'm hearing from you is that security and risk professionals have always had a complex job, but now the complexity is even more intense and their scope is getting ever broader because there's so many more risks in play.

Jacky: I think you're spot on because 10 years ago, somebody who was working in security was probably a fairly IT literate person who was interested in securing technology. And then we introduced the layer of risk that was sitting over that. So, we have professionals who need to understand risk in order to look at which cybersecurity techniques and tactics they're going to use to protect an organisation and where the risks are that they need to focus those. And now we've also put the kind of geopolitical element on top of that. So, your ideal cyber security professional should probably be a techie, a risk professional, great of kind of geopolitical knowledge. They need to know about economics. So, there's many many perspectives that come into somebody who really wants to understand cyber security and what's happening in that space. And what recommendations they should be making to organisations to try and secure themselves a bit better. So, the dynamics are large and growing, and I think we have people who are specialising in each of those different areas, but there always has to be somebody who's having that helicopter view over the top who actually understands the whole dynamics so that they can help orchestrate what the right actions are to do so. I think the job is getting more complicated for sure.

Ellen: Certainly explains why the good ones are never out of a job, and why it's probably a great place to look if you're a young person who wants a very interesting future.

Jacky: Yes, I completely agree with that. I feel I have the best job in the world. It's so interesting. I never have the same day twice. And you get to do really nice things for organisations and help them when they've been attacked and help advise them how not to get attacked. And you actually genuinely feel as if you are doing something for people every day, which is nice.

Ellen: Always good to end on a high note, Jacky. Thanks for joining us today.

Jacky: Thank you for having me.

Ellen: Listeners, if you want to dive deeper into the topic, search Accenture in combination with the words Cyber Resilient CEO and you'll find a recent report on the topic. And if you love the podcast, you know what to do. Please share and review on your favourite podcast platforms so more people can find out about us. Until next time.

Outro: Walk in the Cloud.