INSIDE INNOVATION PODCAST EPISODE 3: CYBERSECURITY: STEPS TO A SAFER VIRTUAL WORLD

AUDIO TRANSCRIPT

Hosts:

Ebunoluwa Ogundipe, Security Consulting Consultant

Robert Downie, Security Delivery Senior Manager

Jane Frankland, Cybersecurity Executive, Author & Keynote Speaker

Ebunoluwa Ogundipe [00:00:03]

Welcome to the third episode in Accenture's Inside Innovation podcast series. My name is Ebunoluwa Ogundipe and I'm a security consultant in our managed security services team at Accenture. I'm here with my colleagues, Robert Downie, who is a security delivery senior manager, in our simulated cyber attack team, as well as being here with Jane Frankland, who is a managing director and leader of our UK Applied Cybersecurity Services at Accenture, as well as being a best-selling author, multiple award winner, the originator of the Insecurity movement and one of the UK's leading authorities in cybersecurity. So, Rob, can you tell us a bit about some of the projects you've worked on within Accenture?

Robert Downie [00:00:50]

The area I work in is simulated cyber attack. So I help run the team in the UK, which carries out simulated cyber attacks against organisations. So organisations come to us and they want us to, in effect, simulate a cyber criminal, for example, trying to attack their organisation so that they can understand where their weaknesses are in their defences and also what needs to be improved. What are the remediations, improvements that need to be made within their organisation to help counter those? So, for example, we do a lot of work with the financial services sector, so banks, insurance providers and so on. And I've been involved a number of projects within Accenture whereby we have, in effect, mimicked a cyber criminal: carried out phishing attacks, tried to exploit weak or vulnerable, internet facing infrastructure — right the way through to social engineering attacks, where we try and engineer situations where we can gain access to their office as an attacker might seek to do. We spend a lot of time understanding the cyber criminal landscape, what's going on in the real world, what are the techniques that are being used, what are the vectors that are being exploited, so that we can best replicate those in a safe, risk managed way.

Ebunoluwa Ogundipe [00:02:09]

I joined Accenture as an analyst and I've also worked on varied projects. I would say one of my most memorable projects I worked on was with an energy client. And my work there were specifically around being a risk assessor and helping them prepare towards an energy audit, which the client had and had controls, risks that they needed to address. So my job was effectively, you know, helping them assessing that and communicating that clearly in order to close those gaps ahead of the audit. So I just thought I'd share that to show that they're very diverse projects that exist within Accenture as a firm.

Jane Frankland [00:02:51]

So that's really interesting, actually, Rob and and Ebun, when it comes to what I'm doing. So I'm effectively, as a managing director, building a business. And I'm working in Applied Cybersecurity Services, which actually includes a number of different things. I think there are about six of them. It's things like data security; cloud security, which is so relevant right now; platform security is another element or area; I've got digital identity; we've got governance, risk and compliance; and then we've got the human factor. So that's incorporating things like phishing.

Ebunoluwa Ogundipe [00:03:27]

So, Jane, can you give us a sense of the scale when we talk about the threat of cybercrime? And are we seeing anything unusual when it comes to the pandemic?

Jane Frankland [00:03:36]

Yeah, absolutely Ebun. Certainly the threat of cybercrime is very, very real. And right now we are seeing about 375 cyber threats being discovered every single minute. And the predicted cost of cybercrime to the world is over 11 million US dollars per minute. Now, to me, that figure is absolutely staggering. It blows my mind every time I say it. And what we're seeing now, we're seeing three popular attacks rising in frequency, sophistication and severity. And the first is ransomware. And this is essentially a form of malware that remotely infects computers, encrypts data and locks out users. And once a cyber criminal gains access to a system, then they can demand a ransom, usually in the form of Bitcoin, to unlock the system and then return any data they hold. Now, this type of attack has surged by about 40% during the covid-19 pandemic. And although it impacts businesses of any sizes and in all sectors, we're seeing cyber criminals go after hospitals, schools, universities and the critical national infrastructure the most. And the reason why is because they're weaker. So they don't have the skills, the cybersecurity skills, and they may also be using complex or legacy IT systems. The second type of attack that we're seeing a rise in frequency is the supply chain attack. And this is where attackers go after vendors so that they can gain access to all of their customers. And right now, around 40% of security breaches in UK businesses come from the supply chain. And seeing attackers use these types of attacks for me is so worrying when we consider open source. And the reason why is because there anyone can contribute to open source software. And it's really hard to gauge who is there to do good and who's there to do bad. And as 90% of components in an application are open source this is a very real threat. And it's why in the past year we've seen these types of attacks using open source software rise a whopping 420%. And then the last type of attack that is growing in frequency is phishing. It's the most popular form of attack. And it's where cyber criminals prey on human vulnerability, by posing as a trusted source and using email or malicious websites to gain information they want. And certainly during the first half of the covid-19 pandemic, we saw phishing attacks rise to a staggering 220%. So those are the most popular forms of attacks and they are rising in sophistication and volume. And cyber criminals are becoming so much more

creative in the way that they are doing this. And they're using some really highly effective marketing and business generation techniques. But for me, what I find interesting, is actually the types of cyber criminals that we have out there. So I'm going to ask Rob, can you tell us more about these cyber criminals? You know, what do they look like? Who are they? Where are they?

Robert Downie [00:06:58]

I guess initially people have this view of, perhaps, cyber criminals as the classic hoodie in a darkened room hunched over a laptop. But what we're seeing is that's quite different from the reality. So the two descriptions almost of cybercrime that we start to use are: cyber dependent crimes, where it's only those sorts of crimes committed by or via computer network, but then also cyber enabled crimes. And this is where these are traditional crimes where the reach or scale is actually increased by these computers. And that's an important one, because what it is doing, in effect, is bringing into the fold a much greater number of cyber criminals. So you're starting to get organised crime groups who perhaps wouldn't have considered cyber crimes as their go-to criminal enterprise, being drawn into it. And in my mind, there are three kind of key driving factors behind this increase. And one of those, obviously, is that money/reward element that you mentioned — 11.4 million dollars a minute. So you've got that immense attraction of the money and reward, and that goes hand-in-hand with the ease and the low risk of it as well. I think it was the World Economic Forum's risk report for 2020 put the detection and prosecution rate to something, like 0.05%. A tiny number of these crimes are actually getting detected and prosecuted. Which means, in effect, that you have such a broad number of cyber criminals or types of criminals getting drawn into cybercrime because it offers that high reward, low risk element. So we're seeing criminals from all walks really getting drawn into it. One of the things, though, I guess this naturally leads to is what we can try and do and how we counter that.

Ebunoluwa Ogundipe [00:08:46]

That's a great question, Rob. You're right. You mentioned technologies evolving. The cyber criminals are becoming more sophisticated. And what that means is, it's obvious that this requires a mix of diverse skill sets to be a cybersecurity professional, and also to stay ahead of the threat landscape with protected organisations. And the skill sets range across different aspects. So, for example, having a meticulous attention to detail, which gives you the ability to spot trends or abnormalities in the behaviour of your organisation's IT systems, or having an analytical and inquisitive approach to problem solving, or, for example, being a great communicator, which can be applicable, for example, in clear articulation of complex concepts or articulating inherent risks and controls in an organisation to your clients. So fundamentally, I would say the skill sets range from soft and technical skills, and they lie in one's ability to learn fast, to grasp new concepts and being able to translate those to value add, that can help protect an organisation. And also, I like to break the myth, that I've oftentimes heard about being from a certain educational background to excel in the cybersecurity industry, or to be a good analyst. Say take me for an example, right? I studied computer engineering as my undergraduate degree but software coding was not my favourite. And I've often heard a number of people say, I'm not a coder, I can't excel in the industry. And I like to use myself as an example because here I am excelling, having worked across various industries like financial services, energy and recently in telecommunications, where I lead a team of cyber security analysts on security detection and protecting my organisation's crown jewels. Jane, I know you've done some excellent work when it comes to women and the cybersecurity industry. Can you tell us about this and tell us what's working?

Jane Frankland [00:10:50]

So my work in this area started a few years ago,

actually, when I wrote a best selling book on women and why a failure to attract and retain women in cyber security is making us all less safe. You see, women do see risk in a different way to men. And researchers have found that women are actually more risk averse than men. It's absolutely fascinating when you look at the research and there have been hundreds of studies that go into this. But it actually turns out that women avoid risk more than men because they are really good at assessing odds. We know that women are highly attuned to changing patterns, and that is a skill that's needed for correctly identifying threat actors and protecting environments. We also know that women typically have high intuition, emotional and social intelligence, and that they're able to make good decisions quickly without having all of the information. Now, the collective intelligence of a group improves by 73% when the numbers of women in it rise. And when you add in age and ethnicity, it increases a further 8%. So women have this ability to impact the environment, impact the way that we are approaching risk and the work that we're doing in cybersecurity. But I'm going to turn a question to Rob now. And what I want to ask you, Rob, is where is the industry going? What are the skills of the future? What do we need to be looking at?

Robert Downie [00:12:18]

There's probably a number of areas. I mean, there's a technology side to this, which I think is important. As you mentioned, you know, the cyber threats themselves are expanding. And it's beyond computers, networked smartphones, those sorts of things. It's the whole Internet of Things now: cars, railways, planes paired with anything with the kind of electronic heartbeat or pulse or whatever — now being connected to the internet becomes a target. So the skill sets are incredibly varied that we're looking for. One of the areas that I find particularly fascinating actually is around AI and its application. What we're seeing, especially in technology solutions now, is the implementation of narrow AI, so to speak, which is the idea of AI being used on a specific data set, a number of data points to try and process that far quicker and better, fundamentally, than humans can. So the role of data scientists and the ability to process and understand big data and how you train AI systems, both from building algorithms, software developers in the skills there, right through to, as I said, cleaning and presenting the data for AI to work on. That's something which I'm fascinated in because it's already found its way into a number of products. But it's an area which, I guess in all walks of life, but it's certainly an area in cybersecurity when there is so much data and there's so many data points have to be processed to look for patterns of bad behaviour or malicious behaviour. It becomes something far more useful. And it's certainly something where we're seeing demand for skills, in terms of being able to work with it.

Jane Frankland [00:13:58]

The only thing I would add is you don't necessarily need to have all of those skills, and I want to make that really clear. So I came into the industry, actually, without a tech background, like so many people in the industry, particularly of my age. So I just want to make it really clear that if you have that ambition to come into the industry and you care about it, then there are ways for you to come into this industry without having all of those skills or without necessarily being 100% pure tech. The other thing I'm going to add is at Accenture, we like to give people plus one jobs as well. So I have a number of plus one roles that I am executing at Accenture. So because I am very well known for the work that I do with women and diversity, I'm strategic advisor for global security. So helping Accenture to really build the diversity in security. I'm also in Accent on Gender in technology. So that means that I dovetail into technology and work on gender and then I'm also a lead for inclusion and diversity within the whole of the UKI practice.

Ebunoluwa Ogundipe [00:15:19]

Absolutely. Thank you for that, Jane. As always, this is something we could talk about at much greater length. But it's been really interesting to dig into some of the challenges that businesses, public services and governments are facing and also the skill sets required for the future of cybersecurity. And it's obvious that cyber is only going to become more important and more urgent in the coming years. And if you'd like to keep pace with that evolving landscape, you'll find a host of resources on our website at Accenture.com. Be sure to get involved in our social channels to share your thoughts and keep up with the latest developments. Thanks again to my colleagues Robert Downie and Jane Frankland for sharing their experience and expertise with us. We hope you've enjoyed it as much as we have. And if you enjoy this podcast and want to hear more, be sure to check out our Powerful Minds podcast series where we talk more about technology's power for good. Cybersecurity is an exciting and fast growing area, as you heard us speak about during this show time. And if you're looking to be part of something really important, check out our website at Accenture.com/careers to find out more.