S5 Ep 2
TITLE
The Cyber World

Participants
Ann Barron-Dicamillo, Global Head of Cyber Operations, Citi
Ann Johnson, CVP & Deputy CISO, Microsoft

Jorian Murray (00:01):

Hello, I'm Jorian Murray, and welcome to Good Things Happen, the show that invites changemakers and enablers to share their inspiring stories of progress. Whilst change can be uncomfortable, unexpected, and at times, disruptive, it's inevitable. And more often than not, change is for good. We'll be hearing from people from all walks of life who have been at the forefront of change, including their journeys to get there and their motivations. Because when people work together for a common cause, good things happen.

Ann Barron-Dicamillo (00:35):

And I think if you want to have a job that you look forward to every day, working in cyber is definitely a career to consider because it is different.

Ann Johnson (00:43):

And you're having an impact on actually everything that people do. People'll use the bank, people going to the ATM, or people going to the grocery store, or the phone calls you make, or your smartphone. All of that has to be secure.

Jorian Murray (01:04):

This October, it's Cyber Security Awareness Month, an initiative launched in the United States to spotlight online information security best practises, and to rally us all to do our bit to combat cyber threat. The size of this threat is reflected in the growth of the cyber security sector. This is a market estimated to reach $268 billion in 2024, and expected to grow to $878 billion by 2034.

(01:37):

To help us navigate this growing threat, we are fortunate to be joined by two experts in their fields, who are both called Ann. As Deputy Chief Information Security Officer at Microsoft, Ann Johnson drives external engagement. A recognised thought leader on cyber security, and sought after global speaker and published author, and specialises in cyber resilience, online fraud, cyber attacks, compliance, and security. Ann is also co-creator and host of the Afternoon Cyber Tea podcast, which you can find on all popular platforms. Ann Barron-Dicamillo is Global Head of Cyber Operations at Citi. Before joining financial services, Ann spent the first 20 years of her career in Washington D.C., in public sector roles, serving as the Director of the United States Computer Emergency Readiness team of the Department of Homeland Security. Welcome to you both, and thank you for joining Good Things Happen.

(02:43):

Microsoft Ann, please tell us your story. How does one become a cyber security expert? Is this something, were you very techie when you were a little girl?

Ann Johnson (02:55):

I was not very techie when I was a little girl. It's funny, I actually, throughout my childhood, and even through undergraduate, had said I was going to go be a lawyer. I wanted to practise international law. I had this whole ambition. And somewhere between graduating from my undergraduate programme, where I have a degree in political science and communication, which is great if you're going to go be a lawyer, somewhere between graduating and actually going to law school... And I'd been accepted, I was ready to go. I just said, "You know what? I want to go work for a few years." I had come from a financially insecure family, and put myself through college, and struggled a bit. So I just said, "I want to go work."

(03:37):

So I moved to Los Angeles, and this was a time when jobs... There were not a lot of jobs, and I literally ended up in technology because I responded... I'm old enough that I responded to a newspaper ad for a floor salesperson in a computer store, in a strip mall, in a suburb of Los Angeles. And that is the inauspicious start to what became a thirty-some odd year technology career.

Jorian Murray (04:04):

I love these inauspicious starts. I think most of us have had them. Ann Barron-Dicamillo, tell us your early years and tell us your journey?

Ann Barron-Dicamillo (04:17):

It's actually very interesting. I didn't realise Ann Johnson's start. It's very similar, actually, which is very interesting. I've always said getting a career in cybersecurity, most of us have very unusual starts to how we have entered into it. And I had a similar background. I had a Bachelor of Arts undergrad education. I actually ended up going to work in Washington D.C., thinking I wanted to go to law school and pursue that route. I worked on the Hill for a few years, and quickly became very disillusioned with politics, and did not want to pursue a career in that side. And I got an extra responsibility. This is the late '90s, mid '90s, late '90s. And the congressman I was working for wanted to set up an HTML web page. And so, here I am, sure, I'll raise my hand, I'll do that.

(05:11):

And at the time, the US Department of Agriculture had a lot of classes you could go and take on web development, HTML development, and other kinds of things. And so I took some classes, I figured out how to do this. And I thought, "This is fun. I actually really enjoy this." Ended up taking some more classes at USDA, and then I applied for a programme at American University, where I ended up getting my information security graduate degree. Pivoted to development work, and I did that for about five plus years. Really enjoyed that, always in D.C., so I had that connection back to politics. You can't live in the city and not have that. And I ended up working at Department of Commerce, where I developed a website and it was Spectrum Management for NTIA. I won an award. It was great. And at the time, they were doing something called information assurance, which was the very beginning of how the government was thinking about cybersecurity standards and applicability to compliance. And so I had just developed this website, and my boss asks me if I want to now compliantly certify it for information assurance.

(06:14):

And so I pivoted over to the reverse engineering side. I think, as a developer, I'd always been the Ford engineer. I looked at it from the perspective of a normal user. And I never really thought about how easy it is to reverse engineer and break these things. And I think, within an hour, I found a cross-site scripting error or something along those lines. And it was just fascinating to me. In all the classes I took, it wasn't really something that was taught to a lot of our software developers. And so I thought, "This is a great space to get into." I got my CSSP, and I've been in cybersecurity now for 25-plus years, and never really looked back. But it is an interesting start to a career. And I think I always learned, take the opportunities that are presented to you because you never know where they're going to go.

Jorian Murray (06:58):

Absolutely. Just while we're talking about starts in this industry, I guess, a business, or a category, that's going to treble in size over the next 10 years, you must be constantly on the lookout for talent. Where and how do you look for talent, and how do you attract them into this world, Ann Johnson?

Ann Johnson (07:20):

Yeah, I think that's a great question. So I started in cyber, similar to Ann, about 24 years ago. And I never intended to stay in the field, and I used my own start. I had done a lot of things. I was, at one point in time, like Ann said, take the opportunities, I was a network architect at one point in time. I was actually an operations manager for a large scale, one of those big box computer resellers for point in time because I was like, "I want to learn operations at scale." So I went and did that. And when the opportunity, a company I was working for was being acquired, I looked at the acquiring company, I said, "I'm not sure this is the right place for me."

(07:59):

We carried this RSA security hardware token with us to log into the VPN for remote access. And I became really fascinated with the technology. So I studied and learned everything I could about how they worked, and the algorithms, and all of those things. And applied for a job at RSA. Why do I tell you all of this? Because it's harder to get into cybersecurity than it was in the year 2000. This is when I started. I knew nothing about cybersecurity, other than I knew how these tokens worked, and I obviously understood passwords. But I really didn't know much about the field. And I learned along the way. I've spent all these years studying, taking every course I could, and just learning cybersecurity.

(08:36):

So now, when I look at talent, I think about my own journey, and I say, "Okay, what are our expectations? What are the actual entry level roles that we can have?" Because there are entry level roles. Not everyone has to have three to five to seven to 10 years of experience. And one of the places I to recruit is, I love to recruit transitioning military members, folks that are transitioning back to the private sector. Because they understand how to work under stress, they understand how to work on a team, and a lot of them have an investigative background. We can teach them cyber skilling. I find myself surrounded by a lot of former military or former law enforcement folks for that reason. I think it's a great place to recruit and to bring talent into the industry, but we have to be willing to invest.

(09:24):

Career changers, I was talking to someone recently who was a chef, and then went back and got a cybersecurity degree, and now wants to pursue a career in cybersecurity. Talk about a high stress job, a chef in a professional kitchen is a very high stress job. So thinking about those intangibles, and how we can actually teach somebody cyber skills, you have to widen your aperture, and then really invest in people. And that's been one of my mantras in the field. But that's how we recruit talent. And it's hard work, and it's very competitive, and the most senior established people can be very expensive. But you have to just go out there and be willing to widen the aperture of the talent you're looking for.

Ann Johnson (10:03):

You have to just go out there and be willing to widen the aperture of the talent you're looking for and be willing to invest in people.

Jorian Murray (10:05):

So you're looking for strength of character and people who can deal with those situations, the technology. I guess technology is changing all the time and therefore you are constantly learning about the technology.

Ann Johnson (10:22):

Correct.

Jorian Murray (10:23):

Ann, tell us about your role at Citi and whilst doing so, you also answer that question about talent and how you find people.

Ann Barron-Dicamillo (10:33):

So a couple of things. I definitely agree with Ann's commentary. I always think of it as being inherently curious is a really great skill to look for in the folks that we're recruiting. I think it is really difficult to find a career those first two to three years out of college. It's probably the hardest job you'll get in cyber. Once you get that experience three to five years, that it becomes much more easier to find your next role. And so I think where we're trying to focus on is how do we help those college graduates? Definitely programmes like Ann mentioned is a great opportunity. I have a son who's actually in the Air Force and so he's trying to figure out which degree he wants to get in. He works in avionics and not in cyber. He thinks, "Oh, I have to have a cyber degree to get a cyber job." And I told him, "No, no, no. There's great opportunities." So I'm very encouraged by what Ann shared. I'll definitely share this podcast with him so he'll know there's a path for him.

Jorian Murray (11:26):

Cool. When I did my research for this, I originally started with the words cyber world and all of my research took me to security and cyber crime and bad actors. Is that fair? Should that dominate? Are there more positive, innovative areas of opportunity that you both work in or are your worlds dominated by cyber security? Ann Johnson.

Ann Johnson (11:58):

It's an interesting question. I'm going to give a parallel in the real world that everyone will understand. Whenever there's some major criminal event, I always get frustrated that we focus so much on the criminal as opposed to focusing on the victim. I want to hear the victim stories. I want to know who the people were. I think the same thing applies in cyber crime. The flashy headlines are, there was this major breach in this major event and then everybody doubles down on, well, who was the actor and the threat actor and what was the motive? When the real story to me is, and I say I'm a cyber optimist, I say this all the time because I know that for every flashy headline and everything you see about a bad actor and everything you see about an intrusion, there's thousands of things that our cyber defenders who are on the front line every single day working hard, they've detected and they've blocked. We stopped the majority of cyber events. It's not perfect. There is no such thing as perfect cyber security, and we like to say that we have to be right all the time. The bad guy only has to be right once. But let's talk about our cyber defenders more. Let's celebrate the hard work they do. Their jobs are extremely difficult. They're trying to reason through a massive data set to figure out what is it that actually makes the company the most vulnerable or the organisation the most vulnerable, and what is it that's going to lead to attack?

(13:25):

I would love if the industry had more of a lens on that and highlighting more of the great work of these folks that sit in SOX and these folks that are in defence and the folks that are doing all the different jobs there are in cybersecurity as opposed to, as you said when you did your research, what comes up is the threat actors and the bad things that happen. Let's celebrate some of the great things that happen every day in cybersecurity.

Jorian Murray (13:48):

I love that. And by doing that, it might make the bad actors think twice about just the force that's working against them. Citi Ann, could you build on that? Can you give us some flavour of the work that you do?

Ann Barron-Dicamillo (14:03):

I feel like an evangelist for cybersecurity as well. A lot of times what I try to do in talking to communities specifically and recruitment, is demystifying what cybersecurity is, which is to the point of what Ann was saying. I think a lot of times there's so many other opportunities within this field besides just the defence side, which is critically important. The pointing into the sphere 24/7 operations is a must for organisations like Citi and the work that they do is critically important. But there's so many other aspects of this field and so many other aspects of what we do in cybersecurity and cyber every day.

(14:37):

I think about the offensive operations, the folks that get to act like hackers. We have 150 ethical hackers as part of my organisation that are constantly looking for vulnerabilities. They're looking for [inaudible 00:14:47] before a bad actor finds that and working with vendors, including firms like Microsoft, to share that, to ensure that we protect the ecosystem. Cyber green kind of initiatives. If we were able to fix something in one place, we can help ensure that protection across. And so there's a lot of aspects of really being part of a team, that's so important.

(15:05):

I think cyber, specifically in finance, is really also an interesting and unique place to work because most of my financial partners in the business, they consider other peers at other financial institutions a competitor, but I call them a competitive mate. Cyber is a place where you have to work across organisations because cyber doesn't have any borders. It doesn't have proprietary brands associated with it, so something that can hit me can also hit a peer. And so having that competitive mate, that network within the community is critically important and is essential for protection of our firms. And so I think it's a place where you get to network with others and you get to

work in information sharing initiatives through industry groups or through technical round tables and being part of a community that is much broader than just on the defence side.

(15:53):

There's so much proactive actions that we're doing and working with tremendous vendors in this space. I don't know if I said this previously, but it's definitely a continuous education field if you're in the cybersecurity space. Whatever you learned yesterday might not help you for tomorrow. And so the aspect of being continually curious and passionate about curiosity is really going to help you be effective here. And keeping up with the evolution of things.

(16:17):

Gen AI is not a cyber tool, but it's definitely got a place in cyber. And so ensuring that the capabilities that are emerging technologies also can be part of an emerging threat. And so looking at it from both lenses and getting in engaged in where industry is headed, it's very exciting. I always say no two days are over the same in cyber, and I think that's why I love it so much.

Jorian Murray (16:36):

Ann Johnson, you're nodding in agreement. Talk to us about the importance of community.

Ann Johnson (16:44):

The community is probably the most important part about cyber. Look, we, Microsoft, talk about our learn-it-all culture. One of the thing reasons I loved cyber is it challenges my brain every day, but that part of challenging your brain is actually reaching out to that community. We have to build an ecosystem and we have it in a lot of places. I'll commend financial services. FS-ISAC is one of the most mature and well-functioning, sharing organisations there is. And the reason is because all of the members are invested. You're going to compete. You're going to compete for customers and you're going to compete every day. But knowing that you're all in this boat together when it comes to defending and sharing threats and sharing early warning and sharing signal and having those relationships and understanding, you can pick up the phone and just, A, when something happens, but maybe you just want to pick up the phone and talk to somebody because you're having a bad day and you want to talk to somebody that understands that you're having a bad day.

(17:38):

The community in cyber is actually really deep. It's really strong. The only downside, it could be a little insular. We're not super friendly to people that aren't in cybersecurity, and we probably need to get better about that so that we can recruit and people feel like, they feel more open to coming to this field. But it is a really, really great community. There's this great sense of community. It's unique in that competitors are very often talking to each other across the world in many different industries. People that can meet, compete are talking to each other and really, really sharing knowledge and learnings and experiences and building. There are friendships. I've been in cyber for 24 years. There are people that I have deep friendships with for 24 years and they're still considered some of my closest friends. It is a wonderful industry.

Jorian Murray (18:24):

Beautiful. From Citi, give us a sense of, let's break this down. How do you break down this big threat? Are there pockets of, can you compartmentalise different forms of cybersecurity?

Ann Barron-Dicamillo (18:45):

So thinking about the emerging threat, I think there's a number of things that are on all of our minds. The first one being third-party risks. Your partners, that we talked about previously, can also be an entry point into your environment. And so I think organisations, you can protect yourself and you can protect your ecosystem and ensure that you've locked down and created the proper controls and all the different aspects associated with your architecture, they alerting, but your third parties, you don't have the visibility into how these organisations are potentially vulnerable to exploitation, how their internal workings are really conducted in a way that would be on par with your own.

(19:30):

You get visibility into them and in different kinds of assessments you do, but it's a one-time review, point in time review. And so there's a lot to be done in the third party space to really focus on continuous monitoring opportunities to really try to implement things that can help mitigate against that risk. I think in the space in general, we have thousands of partners and so that's an area where we pay close attention because we only know what the status of their environment looked like the last time we were on site with them.

Ann Barron-Dicamillo (20:03):

The status of their environment looked like the last time we were on site with them. And so I think that's an emerging threat space that will continue to be one, just because of the lack of visibility that we're going to have in that environment. And also the fact that we've seen threat actors specifically go after a secondary target when they can't get after their primary target. And this is an easier way sometimes for them to get in, and they come in as a credentialed user or a trusted user, and so the access that they have is going to be on par sometimes with their internal users. So it's a big threat area for us that we focus a lot of attention on.

(20:29):

I think the other thing I mentioned previously is just generative AI and what's happening in that space, and deep fakes, and just AI-powered malware. It's amazing how quickly threat actors are embracing technology. I think even the way we used to train our employees on looking for phishing, those cues are no longer there. They're no longer making grammatical errors, they're no longer making some of these mistakes that they made in the past. These emails that they're sending as part of the phishing campaigns look very legitimate, and because of the power of AI and how they're leveraging that to execute things very successfully. And so I think even brute force attacks and how they're leveraging that, and botnets and other kinds of things, how hackers are quickly generating very specific content from how they gather that from social engineering about our users, to really go after weaknesses or looking at designing malware that can avoid detection. They know our tools, they know what we we've deployed, and they know how to reverse engineer those tools to bypass those controls.

(21:32):

And so all of that is giving the attacker an advantage, and so we have to ensure that we are, again, partnering with others, staying ahead of the things we see in that space. And then the last one I would bring up is really just quantum computing. I had the privilege of speaking with some folks from NIST last week around where this is going in general, and I think every time I have a conversation with them, I get more concerned about how quickly the power of quantum is powering the ability to break a lot of the encryption capabilities that we all rely upon, and what does that mean for us? And we have things like steal now, decrypt later kind of campaigns that I think in the past, there was a lot of, "Oh, well, it's encrypted data. We don't have to worry about that." Well, that's no longer the case because that data can be decrypted with the pace we're seeing in a quantum space. So I think it's changed the way we respond to some of these events as well.

(22:28):

So those are just some areas, I think the last one, actually, I'll just say one more that I think is very fascinating today, specifically as an election year, I think 60% of the population, 80 countries, 60% of the population went to the polls this year are going to go to the polls. And that really leads to what I would consider to be geopolitical risks, this increased tension, numerous flashpoints for conflict, ongoing wars. There's an aspect of cyber that can feed into geopolitical risk. And so I think that's something that we're working on, and really ensuring that we have visibility into these potential global situations that can have an impact on financial institutions. Working with partners and government and partners across the firm that have global footprints, and where the touch points of the geopolitical risk can really have an impact in your business operations.

Jorian Murray (23:19):

Anne Johnson, listening to your excellent podcast, you talk about thinking one step ahead. It feels a bit like a catchphrase for your show. How does one do that with generative Ai? That's changing the game completely, is it?
Ann Johnson (23:40):

Yeah. So yeah, I often say, because I'm a big ice hockey fan, "Skating to where the puck is going," quoting The Great One. But we in cyber have to always be aware. And Ann highlighted a lot of areas for emerging threats and emerging risks and things that are coming very quickly. I do believe, because we've been thinking about AI and cybersecurity defence, and I'll talk about that part of AI, not necessarily the security of AI, but actually AI as part of cybersecurity defence, we've been thinking about this for years. This isn't new. As machine learning became more sophisticated, as AI became prevalent, there's a couple things that occur to me. One is that our ability, I talk a lot about IoT and OT defence because our ability to actually understand what a device is or a class of device is, even if we've never seen it before, AI can tell us, because a device only makes certain calls. And it's purpose-built to do certain things, so AI should be able to reason through that pretty quickly and say, "This device isn't operating as expected," even if you've never seen the device before.

(24:40):

The same with service identities, machine identities, human identities. I fundamentally believe that we are ahead of the curve from the AI defence standpoint and understanding. The actors obviously are picking up very quickly. They're obviously going to be using AI to accelerate attacks, merge that with quantum, and you have a different paradigm that we're going to have to defend against because it's going to be faster, it's going to be more sophisticated. They're going to have more intelligence to work with very quickly. But our ability to improve the operations of our security operation centre, think about the fact that Microsoft, we see something like, I think the number's 78 trillion threats a day or something like that. We see 78 trillion signals a day that could be something, or maybe nothing. No human can reason over that.

(25:25):

So machine learning, and then AI, is going to give us the capability to reason over that data very quickly, to eliminate what's pure junk, to then figure out what are the most important things, and give our cyber defenders a fighting chance. Because it could say, "Look, Mr. or Ms. Cyber Operator, here are the top 10 things you need to worry about, and by the way, we're going to automate response to a bunch of stuff because that's important. But the 10 things you must worry about, here's our recommended next best step, or here's what we can do to automate it." That's going to give us a much, much better chance of detecting very quickly that an actor is in our environment, containing them, mitigating the damage quickly by putting them in a box someplace, and then ultimately evicting them.

(26:05):

So I do believe there's a big promise for AI from a cyber defence standpoint. We're in the very early days of it. We're also in the early days of seeing actors exploit and abuse AI. My nightmare scenario, I will tell you, and the thing that I worry about regularly, and we have to continue to work on defending against, is malware that becomes adaptive in the wild. We see it at the front door, we say, "Okay, we can defend against that," but it actually knows what the defences are and it starts to adapt itself. That is my nightmare scenario, and what I think automation and AI, and even quantum will accelerate that, and what we as defenders have to be planning for. But we're really good at planning. And we will keep being really good at planning. We're really good as a collective community, taking these modern technologies and building them into defence systems, and we're just going to have to continue to stay one step ahead of the actor in doing that.
Jorian Murray (26:55):

And it's not just planning, you mentioned when we first met, war gaming exercises. Tell us more about that.
Ann Johnson (27:04):

Well, every organisation I know does tabletops, right? They do tabletop exercises throughout the organisation. They do them not just for cyber security, but for also other types of events, other types of resilience or natural disaster operational type events. From a cyber standpoint, you really need to have those exercises in a lot of

different places. You need your cyber defenders doing that war gaming cyber defence. You need your executives, including your board, doing tabletop exercises related to cyber security. I think it's incredibly important to set up a scenario that, if you cannot communicate, I'll just use one example, let's say your email system is down because a cyber actor... You know that it's been infiltrated by a cyber actor. How are you going to communicate that?

(27:44):

That is both a resilience scenario and a cyber scenario that we need to plan out for. So those are the types of tabletop exercises, understanding what could have broad impact on your enterprise, doing tabletop exercises and making sure not only that you have a technology plan, you have a communications plan, you have a plan for how you're going to talk to your regulators, your legal team, human resources, external communications with customers or partners, media. All of that has to be included in these tabletop exercises. And you have to make the plan, and then you have to test the plan, and then you have to tabletop the plan repeatedly so that... You don't want people making hard decisions during times of crisis. You want them following up playbook during times of crisis. And that's why you have to have these exercises so people know exactly what actions they're going to take if there's a crisis.

Jorian Murray (28:32):

And at Citi, how do you effectively communicate? Because I guess I have seen communication in my career, and sometimes it can feel a bit like a distress purchase that you, "Oh, it's not going to happen to me, and I'm going to just ignore it." And how do you get people motivated and engaged to really understand the drama and the power and excitement of what it is you do?

Ann Barron-Dicamillo (28:58):

To follow on what Ann stated, I think it's really exercising those plans. Because we all have playbooks associated with a crisis management situation, and we want to make sure, across a lot of different crises that can happen in a firm, cyber is one element of that, at the end of the day, we want to make sure that our businesses, our regional leaders, our global leaders, that they're prepared to communicate to a number of different audiences, customers, clients, peers, regulators, and understanding the cadence of those communications. There's a lot of regulatory communications that have to happen on a certain timeframe. So we want to make sure that we understand when that communication has to happen.

(29:37):

And that all goes back into the cyber exercises that we do across the organisation to include our executive management team on our board, making sure that they're ready, they know their roles, and we want to make no assumptions. I think Anne said it really well, you don't want to pull out your playbook in the middle of a crisis. Because at that point, it's too late, and trying to make phone calls or connect with different folks that you're going to need during an event-

Ann Barron-Dicamillo (30:03):

Make phone calls or connect with different folks that you're going to need during an event. You want to have those relationships ahead of time and you want to make sure you know who's on point to conduct that kind of outreach as well. The cyber teams do a great job of really making the events really real-world-like. We want to make sure the scenarios are intelligence-led, they're driven by things that we've seen in the industry. And then bringing that back into our firm to say, "Okay, how would we respond to something like that? What's the takeaways that we can have?" And I think that's the other important part, is it's not just an exercise, but it's the after action plan associated with that. What can we do? What are the lessons learned from this and how can we improve our crisis management response at all the different levels? Because there's going to be a bad day that's going to happen to firms and we want to make sure whether it's internal to the city or one of our third parties, that we know how to respond. We know who has the ball, we know who to connect with, and that that's all part of the plan.

(30:56):

Practising for a bad day is worth a pound. When you're in a bad day and have not to practise, it is just, it's being behind the ball in a way that you'll never catch up. And it leads to a lot of distrust, I think, across those communities as well because you can have inconsistent communication or changing your statements. And so the

last thing you want to do is find yourself in a situation like that as well. So practise makes perfect. Do it on the regular. Make sure that you've got your senior leaders engaged, because a lot of times they're the ones that are going to have to make those decisions to make those calls.

Jorian Murray (31:32):

Last question to finish off to each of you. I'd love each of you to give a short pitch to young talent who might not previously have ever thought that this was a career that might be for them. You make it sound fascinating, and I think one of you said every day is different. So yeah, Ann Johnson, you go first. Why should some smart young grads be looking to your world to pursue a career?

Ann Johnson (32:03):

Yeah. I would say a couple things. One, it's very mission driven, so you're actually making the world safer. You're actually doing something that's incredibly meaningful every day, even if it can get to be a bit of drudgery occasionally. You're still doing something that's incredibly meaningful every single day. Number two, you're exercising your brain and you're exercising it differently every day. So the ability to challenge yourself to be better, to learn more, to engage with really smart people.

(32:28):

You're also working with this amazing community and these amazing people. Cyber people are exceptional human beings. I'm very biassed, but cyber people are exceptional human beings because we're all on this mission together. And then it's just fun. Believe it or not, it's fun. I know it. Some days it can feel like it's really unfun, but it's actually a really fun place to be. Because you're solving hard problems and you're solving hard problems with great people, and you're having an impact on actually everything that people do. People who use the bank, people going to the ATM. Or people going to the grocery store. Or the phone calls you make or your smartphone. All of that has to be secure. So you're impacting the entire ecosystem of the world. Just think about that.

Jorian Murray (33:11):

Wow. Follow that, Ann.

Ann Barron-Dicamillo (33:13):

I was just going to say... I would add to that. I think the benefit of working in a cyber field is you get to work across with partners across the organisation. Cyber is a team sport, and so for us to be successful in what we're doing, we have to partner with our business partners, to partner our legal folks. To privacy, to work with our compliance folks. To work externally with our peers and with our vendors, and working with US government or other government entities, both regulatory as well as other sides. You have this opportunity to work with so many different individuals in this field because it is a collective, for us to be successful. I think Ann said it really well. It's a fun place to work.

(33:55):

I think if you want to have a job that you look forward to every day, working in cyber is definitely a career to consider because it is different. You're going to be faced with different challenges. You are working against a very sophisticated adversary. And you're really trying to ensure that the decisions that you're making are going to stay ahead of that adversary. Getting into predictive analytics and working with emerging technology and really getting to think about problem solving and applying that every day to your work. It's very fulfilling, and it's also being part of a team that is really just intelligent and motivated, passionate people. And I think that breeds the same in yourself as well. Being with people that are very passionate about the work really empowers me and influences me to be a convener of others, to try to encourage. And be really passionate and excited about what we do in our field. It makes a difference, and you can see the impact of your work.

(35:07):

Sometimes the impact of your work is a negative, meaning that you don't get to, you don't see an attack that didn't happen. But you can look at those statistics and see all the things that you were able to prevent, and that's also extremely impactful. And so it just, it's a career where you also can set your own path in it. There's just so many different opportunities that you can do as well. And it can be irrespective of what you're doing today, moving into

another aspect of the organisation. And also I think there's a lot of ability to move into the business and back into tech as well, within this field as well. And so it's very unique in that you can set your own career path based on your interest and ensure that continuing education aspect.

Jorian Murray (35:52):

Wonderful. Compelling answers, compelling conversation. Thank you so much. I know we've just scratched the surface, but I feel so much more informed and energised about the work that you do, and thank you both for doing it. I'm sure you're protecting me somehow, and I don't even know how, but thank you for coming on to Good Things Happened. I've really enjoyed the conversation.

Ann Johnson (36:17):

Thank you so much.

Ann Barron-Dicamillo (36:17):

Thanks, Ann.

Ann Johnson (36:38):

Thank you. Ann.