sonix

NAME

IT Interview.mp4

DATE

July 12, 2020

DURATION

47m 26s

4 SPEAKERS

Samantha Gloede
Ben Matthews
Andrew Moloney
Helen Nowlan

START OF TRANSCRIPT

[00:00:00] Samantha Gloede

So I work at KPMG, which is one of the big four consulting and audit advisory firms. And I've been with KPMG for 22 years, so I'm probably older than like a lot of people in this team. And so I started I went to Murdoch University in Perth and I did a commerce degree with a double major in computer science and accounting. And at the time, (I graduated in like ninety-eight) so I was going through like recruiting sort of stuff for internships a couple of years before that, and I saw some ads from my so my competitors like KPMG, PricewaterhouseCoopers, Ernst & Young and Deloitte. And at the time there were six of us. And they've you know, there's been acquisitions and they've joined together. So now there's four of us. And I at the time, it was like not very common to have a business degree combined with any kind of technology degree. And I credit our mum for suggesting that I do that, she was like, I don't know why, but I think something to do with computers. You're really good at it, and I feel like it's the way of the future. So I went ahead and did the computer science double major. And at the time the big consulting firms were really interested in getting people that could understand business, but also, could understand IT and throughout my career, I think that the value proposition there has been, if you can help business people understand technology and how it helps to drive and enable a business, and it's becoming more and more important as new technologies are coming in. And really nowadays, people that work in business have to have a foundational education in technology, and I know certainly that often, but most of our clients, they typically don't recruit people now that don't have a technology credential of some sort, because you have to be able to understand and operate with technology. So I started I did internships at all. And I started I did a couple of summer internships and just started at KPMG and haven't gone back. Twenty two years later, I don't feel like it's been the same job. I've worked, I've worked in Sydney. I've worked in I've lived and worked in the United States of New York. I've spent a ton of time in Asia, in all of the countries. When I was living in Perth and Sydney, I had an ASPAC role. So I went and met clients and did a lot of work across the region. Now that I'm in a global role, I have clients in the US, in Europe, in Asia. I kind of work all over the place, and why I thought that it would be interesting to talk to you guys, So I do technology consulting and it's focused more on technology risk. So it's cyber security. It's all of the other risks that exist that Technology can either control and manage or that technology introduce us to a business. And we do all of those things. And more and more these days, technology risk is less about fixing stuff that goes wrong, but more involved in the strategy and design stage of any big project, because you have to have an understanding of technology and how to implement it in a secure and integral way to drive successful business implementation. So it's becoming more and more important. So I focus on technology risk. But at KPMG, our technology consultants to everything from the risk side that I do to actual implementations of technology. So implementing an Oracle system for the finance function or workday for the H.R. function so big like ERP implementations for big organizations we do. We have data scientists that do data and analytics are now data is you (sorry I sound American) data is in everything that any organization in, in anything that anyone does and that the value from that data comes from like analyzing it, using cognitive technologies like artificial intelligence, machine learning to run routines like in real time over that data and create insight. So we have people that do that. And all of those things our group are participating in that, because you need to make sure that there's integrity in the outputs, you have to make sure that there's security and that the data isn't accessed by people that it shouldn't. It's ethical constraints as well. When you're looking at algorithms that are run on data, you want to make sure that they know there's no bias around gender or race or religion or. Geographical location. Anything else? It could be any kind of fire. So there's a lot of stuff that we do in technology, and so I thought it would be interesting because we have exposure to all of the components of technology roles at our clients. So I thought I could answer - I know when I saw the overview of your assignment, It's talking a lot about like what could your job be in technology? And I think it can be anything from like working on a help desk to help people with tactical I.T. issues.

It could be actually being the engineer or the architect That's like connecting hardware to implement it. It could be the architects that are designing how that technology fits together and how it supports the business. It could be the business strategists that think about this as is what I need our business to do. And this is how the technology is going to support us doing that. It could be the cyber security. It could be the data and analytics engineers and data scientists. Is this like so many different things that you can do in technology? So I thought I could probably answer pretty much most questions about the different types of roles. And also, when I saw the list of the technologies that were in your assignment. I've done work with almost all of them. So I'd love if you've got questions and it doesn't even have to be on the video. Now, like, if you have questions in the next few weeks as you're doing it, I can talk about like how those technologies are typically used by organizations and it's different depending on the industry that the organization works in. But I can kind of help you guys understand, how those technologies are used in everyday life. So they're amazing.

[00:07:23] Ben Matthews
Andrew, Helen Do you guys have questions? I certainly got a few, but I'll wait.

[00:07:34]

[00:07:35] Andrew Moloney
Oh, not now. I'm I'm happy just to run with what you guys have got. Yeah.

[00:07:42] Helen Nowlan
Theres a couple

[00:07:47] Ben Matthews
While Helen's finding something. Yeah. So, I mean, you've obviously worked those across so many different facets of tech business. Well, it's really, really exciting. I mean, I'm curious about things like you mentioned, bias in algorithms and all the rest of it and what I can do to skew data. Oh, yeah. Rather like is that something that is common where algorithms actually do have, you know, just maybe like they're not really fully considered or something.

[00:08:18] Samantha Gloede
Yeah. So I think it's unintentionally common. I don't think anyone ever. I think for the most case, they're designed in a way that's intended to do what they're meant to do. However, there are some scenarios where people like bad actors can leverage that influence that they have to get the answers that they want to get to give it almost in like sort of a propaganda kind of way. If they want to say, well, this is what the data says and it's and it benefits that business. Right. So we always go in with the expectation that algorithms are written and designed for the best case output in a fair and integrity driven way, but there's many examples where it isn't done in that way and they are easily manipulated. The other thing is that machine learning is just that. It's about machines learning the rhythms, the routines, the personalities, the activities and the actions of the of the data that they are running on and the people the uses of that data. So you'll find that algorithms in the early days are possibly not as accurate or as broad in their access as they will be maybe in a month down the track or, you know, some sort of longer duration. But we have a solution that we have partnered with IBM, one side IBM provide the technology and we provide the data scientists and the consultants who can analyze the outputs, and we call it AI in control and like jokew word we don't give to the general public is "bots gone wild" because they actually really can go wild, either intentionally or unintentionally. So we have this solution that we built with IBM where basically we in input parameters into the IBM system that will analyze the algorithm to make sure that there's integrity so that there is completeness and accuracy in what it's doing, that it's free from bias. So it could be any of those things I mentioned before, it could be gender based, religion based, geographically based, politically based, like anything. And also that, fairness so that that output's are fair based on what has gone in, where the data's come from and that it's been sourced in a fair way, so an algorithm could be running perfectly well with complete integrity. But if the source data is kind of dicey, then the output won't be a fair response. So they're the sort of solutions that we create to help check on that sort of stuff.

[00:11:27] Ben Matthews
Amazing, and so in that sense, do you essentially apply a machine learning to scan the algorithm themselves, is that kind of the process.

[00:11:35] Samantha Gloede
We kind of do. So we will - the system that IBM created allows us to input parameters that we think it needs to be checked against because it could depend. Is it a life sciences company or a pharmaceutical company that's creating a covert vaccine right now and using data to do that? Is it a bank that is worried about credit risk right now because everyone's lost their job and they can't pay the credit card?

[00:12:03] Helen Nowlan
I was going to say to you is COVID having a huge impact in this area.

[00:12:08] Samantha Gloede

Huge, huge huge huge on everything. On absolutely everything. So we've done a lot of pivoting in what we do right now to make sure that we are only really investing in and taking solutions to market that our clients are going to need because of COVID. So it depends on on the industry. So I have worked across many industries in the past, but right now I'm focused on life sciences. So that's pharmaceutical companies, medical device. So anything to do with, like diagnostics, so testing, that sort of stuff. And in our space, there's a lot of things that are critical right now for them because of COVID. It's about the security of the IP, but also the physical location where they are testing people's COVID tests, where they're researching treatments and vaccinations. It's very, very competitive. So there's a lot of like cyber risk related to that right now because hackers want to get in and see what is the recipe for this vaccination that this company is is doing versus another. Right. So that's one thing. Another thing that's a really big issue right now across many industries, not just life sciences is supply chain. So we're very dependent, certainly in the US. But I think across most of the world, very dependent on supply chain in China. And it could be production of materials. It could be the raw ingredients that are produced somewhere else. It could be, you know, all of that. Right. We get Iphones and Ipads at a cheap price because they're made in China. But there's a lot of political unrest with that right now, and so what we're seeing is a lot of our clients have supply chain risk where they either can't source it from where they sourced it before, and that drives supply volume issues and price issues, but also because there's so much demand for products that they never needed before, like face masks and gloves and shields and syringes and everything that the whole world needs, they've had to really quickly pivot to figure out how on earth are we going to produce these things in a way that we're not dependent on China. So that has implications across every organization and from KPMG's perspective, it's not just technology, we actually have people that deal with like optimizing that process. From a technology standpoint, we can help with the resilience of the technology that supports the supply chain. We can help with the security of the supply chain. So you to say like these are a few examples where it just shows technology is the foundation of everything that every organization does. Another one is in the U.S. and I think it happened a bit in Australia, too. But they had this three trillion dollar government stimulus package where organizations, small businesses could apply for a loan to keep paying their employees while they could have work. And so we KPMG helped a lot of these big banks processing all of the applications, doing assessments on like potential fraud of the applications because there's people applying for it that shouldn't have applied for it. So all of these things and it's like super interesting. And I, I, I thought it would be cool to talk about this stuff with you guys, because sometimes I know when I was at uni studying I.T., I kind of thought well all I'll do is I'll go and work in an I.T. department. And that's certainly a very, very good offer opportunity. But I don't want you to all think like that's all you can do because you could go and work in like a full on business and your technology will be an integral part of that. So like the big banks will have, you know, the bank is at the front that are dealing with the clients. But in every business unit of the bank, this Technologist's, they're working with people in the front office to help them do what they do. So I think it's super exciting. I'm a nerd

[00:16:27] Ben Matthews
I love it. I really like all things IT and business and how it all intersects. I get the impression that part of why you're so engaged by it is because it's so varied.

[00:16:43] Samantha Gloede
It is. I've never been bored.

[00:16:46] Ben Matthews
It's like not only is it varied, but it's not just like you just jump from these kind of menial tasks to another menial tasks like everything. You know, it's multifaceted and really engaging as well. So yeah, yeah, yeah, yeah, yeah. Really cool. So I mean, what is that something that you love about your job is having the opportunity for constantly varied engagement and working with clients from different locations and constantly suiting different needs and all the rest of it.

[00:17:15] Samantha Gloede
Yeah, that definitely appealed to me because I even I've been there 22 years. I don't feel like it's been the same job. I've worked in so many different places. I've worked in so many different types of roles. But the foundation has always been kind of technology risk. And that's what I do. I mean, I'm very biased. I think working in a consulting firm particularly one of the big four because they're so grounded in like a brand recognition around, like trust and business process. Like, we really know what we're doing. I think that's a really good option because you can really do anything if you decide, like you get really good training up front. You get a really good foundation for three years if you decide I don't want to do this consulting business any more. Going to a bank or any other organization after working at the firm KPMG. It's it speaks a lot on the resume. Because they know you've had really solid training. You've had exposure to different industries, to different functions. So we have people that work in specifically in an industry. So I'm life sciences, we have people in banking, we have people in consumer and retail. We have people in technology and media. And we have people in healthcare. We have people in government and defense and energy and natural resources. So the big mining companies and the big energy companies, so we can kind of work in any industry that you have an interest in. But also you can switch between the functions so you might decide to specialize in finance or in H.R. or marketing or tech I.T. or cyber and you can do all of that stuff and it just completely changes. You know, you don't feel like you're doing the same job. But at the same time, like as a business, we also have a very, very, very big technology organization that support us in what we do. So we have our own CISO who manages cyber security for our business, which is also really, really important because we have very sensitive access to information. We have our own CIO who and chief data officer who drives the strategy for

our firm globally around like what hardware are we going to use? What software are we going to use? What how do we support, you know, a couple hundred thousand people across the globe, like traveling and working remotely? That's another thing right now with COVID, because everybody's working away from the office, working remotely from a technology standpoint, like it's a big issue because they need to ensure availability of the technology so people don't have downtime when they're working from home. So if you've got. You know, an organization that has like 20000 people that used to work in the office on those like hardwired service and an Internet access that was in their office, and now they're all working from home from God knows where. Yeah. How do you make sure that I've got availability of the technology to do that job? How do you make sure that this its secure like theres So many different components to that. And that's a lot of the stuff we're during for clients right now is helping them with remote access to make sure that their workforce to keep working.

[00:20:43] Ben Matthews
Yeah, yeah, yeah. That'd be massive one. We've actually just been reading a little bit about, like, you know, the whole bring your own device to work kind of mentality and what that means for things like cost to the business and security. Mm hmm.

[00:21:00] Andrew Moloney
Yeah, I did have mentioned in regards to the security from your client's perspective. What about KPMG?

[00:21:09] Samantha Gloede
Yes. It's important for two fronts. So we have an enormous risk management function in our business, so we our firm has three functions, audit. So that's the external audit of any big organization that has to report to shareholders. Right. So they do a financial audit. That's a big part. The second is our tax business. So they do anything related to tax. And it's not just like the year end on quarterly tax. It's like very significant, like, you know, understanding if you want to build a supply chain and source stuff from one part of the world that has big tax benefits or not. Right. So they do a lot of that complex tax structuring stuff. And then we have our advisory business, which is our consulting business where I sit. So we have a lot of restrictions ourselves. So I can't work on anything for an audit client in a consulting capacity because there would be independence concerns that we might have access to financial information that we could use to benefit other shareholders or whatever. Right. So there's this big segregation there. But with that comes with you know bad actors have people that might hack or do bad things. They know that we have access to really sensitive data. We can. We have access to financial information. And our clients have really big down to not so big, but like the biggest in Australia, like the biggest banks are our clients. The biggest pharma, like all of the big clients are ours. So if anyone wanted to get access to really sensitive information we have, that's there's a lot of security requirements from a technology standpoint. And we have to when we go through an engagement acceptance for every single job I do, we have to like agree that we're not going to take certain data from the client onto our laptops. And if we do, it is it's like so, you know, we use Microsoft teams for our virtual meetings right now and we are not allowed to like type of client name into the chat. Right. Because so there's of behavioral restrictions, but also as security people have to enforce a lot of technology restrictions on what how we can share information like we're not allowed to use Dropbox when I'm allowed to use Icloud, we're not allowed to access a G mail account on our work computer. Right. So there's a lot of restrictions there. But also theres restrictions in the way that we contract with our clients so that they have to agree to to what they will allow us to access and agree to those restrictions. So it's not just on us, but the responsibility of a CISO So the chief information security officer for us is just as important as it would be for the Commonwealth Bank or example,

[00:24:12] Ben Matthews
Probably more important cause you would have multiple banks.

[00:24:20] Helen Nowlan
Johnny Had a question Ill just ask that. How do you see your field developing in the future? Do you expect many changes as technology improves or processes becomes automated?

[00:24:32] Samantha Gloede
I think that's a great question. I think in my career, we are more valued now than we've ever been. So it's very exciting. And not just within our firm, but like what we do for our clients is much more strategic. Now, I think, like 10, 15 years ago. We were more like the fixing thing. It was like the boring stuff that they didn't really want. It's not that sexy, like doing what we did. Now they involve us right up front in, like, C level discussions. I think one of the maybe I didn't send it through, but we did a CEO sent a CIO survey. But we did a CEO survey of like, I don't know, fifteen hundred CEOs of clients around the world that we work for and technology is like in the top aspects of technology, a probably like the majority of their top five concerns. So it's really important for them. I also think that the expansion of disruptive and emerging technologies like artificial intelligence, machine learning, block chain and crypto currencies, cloud connected devices like all of those things are being used more and more and more by organizations to disrupt and change and transform the way that they operate that Now we are becoming even more important, not and not just make KPMG. I mean, like the technologists that implement this for our clients are becoming much more important because nobody else really understands what these technologies do and how they can help drive value for the business. And it's so competitive these days that these organizations don't automate and digitize the way they operate, whether it be with the customers or the way that they operate that business with

their employees and everything in between, then they're going to lose money. They are going to lose customers. They're going to be taken over by other people. So these technologies are becoming. So so, so, so important, really.

[00:26:47] Helen Nowlan
From a cyber security point, do you find that you tend to be reactive to hackers or do you stay a step ahead of them?

[00:26:59] Samantha Gloede
That's a great question to so Historically, we were more reactive and there's definitely a piece of what we do that has to be reactive. So something will happen and you have to fix it. But the value for Any organization in this security organization now, if they call it security by design. So you want to design your technology architecture so that it's secure from the outset because it's better to prevent these things than resolve them. So there's that element of designing a better security architecture up front, and that's part of the Cyber organization. But also now the exciting thing is you can use technologies like artificial intelligence, like I say, cognitive technologies that artificial intelligence, machine learning, any of those sort of things. You can and we do a lot of this work with our clients where we show them how they could create those technologies on top of what they do to better anticipate something happening. So now most organizations and I'm sure any of the people you work for or with. Now, whatever jobs you have to today as well as your university? I would have some sort of cognitive technology that is scanning absolutely every interaction and digital fingerprint that exists anywhere, whether it's an email, whether it's someone logging into a portal, whether it's an employee that works there, that's like looking on a Web site that is not related to what they do or is not. Theres algorithms that help organizations understand have we got what they call an insider threat. Sois there someone working within our organization that's potentially going to hack or provide access to a hacker externally or they are outside threats that we can anticipated And this stuff is all automated and it's all happening without any of us knowing. That's why I have two phones, because I know KPMG can see absolutely every single thing I do on my personal phone That's why I have two now And It's becoming more and more important to anticipate and predict risk than to fix it at the end, because if, if and if an incident happens, then theres reputational damage, this financial damage. And it's really hard to come back from that. So the preference is to just anticipate.

[00:29:49] Helen Nowlan
So there might be a fine line between risk and privacy. Saying that you have to have two phones.

[00:29:58] Samantha Gloede
Yeah, right, sir. I know as an employee of KPMG, but I sign when I Every year do my declaration I give them . I know that they have access to my phone and my computer and I have every right to right?. It's my choice to use that for personal use or not. But I know that they can access it as a consumer I think the privacy side is like super interesting. Already talked you about that. So there's a couple of big regulations. So in Europe, it's GDPR I don't know if you've heard of that. The general data privacy regulation and then in the United States, they're starting to do it by state. So the first one that happened was in California, it's called the California Consumer Privacy Act, and every state is starting to define their own regulations. And basically, that's that's protecting consumers now. So every organization that has access to a consumer information has to inform them of how they are using it and inform them if there's any potential risk to that. And if they don't really strictly abide by these regulations there's significant financial penalty. So the European one in GDPR There was definitely penalty, but it was more like process related. Whereas in the U.S., it's financial. So if you are in California, if you're a California resident as a person or a resident as a business, and if you find out that your data, either your company or your personal data has been exposed or misappropriated in any way, you can seek financial remuneration. So for every instance for a person its seven hundred and fifty dollars and every instance for an organization, it's like seven and a half thousand by instance It could be they have your name, your state, your address, your credit card. And they used it inappropriately like 50 times. Then you get 750 dollars times 50. Right. So organizations to make sure that they have privacy controls. And and that's not just control. It's like how they organize the whole data, like they spending with us. I mean, my client that I'm working on right now, we're at about, I dont know six million dollars already in helping them work through that. So its significant risk and significant costs, it's very, very important. And it's just you have to kind of think of it through the lens of whether it's an employee that agrees to use technology in a certain way or a consumer who assumes that they can trust an organization that they are engaging with. So much to talk about.

[00:32:59] Andrew Moloney
Very, very knowledgeable of the thing you look with.

[00:33:02] Ben Matthews
We're coming up to like the 40, 45 minute mark in terms like an official interview and all the rest of it. Really doing that. But if you like, you go and spend some time with family after a hard week and all the rest of it

[00:33:15] Samantha Gloede
It's okay. I've got another call in like 20 minutes. But I am I just the other thing I thought I would mention is that I know in the list There were different technologies and which one of been has received blockchain and

cryptocurrency.

[00:33:33] Andrew Moloney
Im so sorry my internet keeps dropping out.

[00:33:36] Samantha Gloede
That's alright. I just wanted to, I might give you like a quick synopsis, but then if you want to ask questions, you can email me. blockchain and cryptocurrency is like super, super confusing even for us And also the regulators, they don't really understand what it is and how to it and all of that. So I thought I would just give a couple of examples of how it can be used to maybe help you understand, like what it is and why it's used. So blockchain I'm going to try and explain this in like the simplest terms. It's basically like a database technology that removes any ability to change or erase records. So there's no way, if something is submitted through a block chain that anybody can ever change its lineage. It started here. It's here now. Nothing can be modified. So there's a real, like ability to trace data and where it goes. And the reason that that's really important. Sorry I'll talk about a couple of industry use cases. For in Australia blockchain we do a lot of work in blockchain with like agriculture and the food supply chain and wineries. Because basically every single ingredient into a food that ends up on the grocery shelf or organic produce that's come from a farm that then goes through different traces or the wheat that ends up in. There's a lot of value in organizations being able to prove the lineage of that supply chain. So that's one of the use cases there in the U.S. theres a there'sregulation called the Drugs Supply Chain Security Act, and it doesn't enforce the use of blockchain but blockchain is really the only way that any pharmaceutical company can actually real realistically like comply to this regulation. So a blockchain technology is used to basically show the flow of every ingredient that goes into a drug, that goes into a lab that is created, that gets sent to a pharmacy, that gets sent to a doctor, that gets injected into a patient. So there's no it's sort of reducing Any counterfeit drugs? It's reducing the ability for doctors to be prescribing people to go to like multiple doctors and get multiple prescriptions of the same thing. And then one other use cases, like in the luxury goods industry. So in France, we do a lot of work with Louis Vuitton, right, in Hennessy. And so they are in like the champagne business, the designer goods business. And it's a big business to copy and have counterfeit items in the luxury business. So they have adopted a blockchain to basically trace their entire supply chain from the goods right through to the consumer. So theres a lot of like implications of that is a lot of risk is a lot of like technology ability to implement a blockchain. But I just thought that might help you guys understand outside of, like, the Big Term. I mean, I remember when I first started working with it I was like, I've got no idea what this thing is and what it does.

[00:37:15] Andrew Moloney
That was really that was a really great explanation as well. And while I've been researching it through doing this assignment all the. Sort of the category with blockchain and crypto currencies, but I want to not harp on about Bitcoin. So through my research Well, I signed off on a case study on pharmaceuticals. I'm sorry, I was just saying that during my research I did stumble upon the case study using like pharmaceuticals and tracking pharmaceuticals and counterfeit drugs. Yet another thing I stumbled on was using it for voting.

[00:37:58] Samantha Gloede
Yeah, anything you want. Like, no doubt about who has access to where it's come from. It's like the perfect. So I've said that over here, like the US election is happening in November And the system here is just like so antiquated And it's so. So rife for fraud. And, you know, regardless if Trump or Biden wins, there's no doubt because nobody can go and vote in person. Whoever wins and whoever loses is going to have some issue around, like the traceability and the integrity of the voting system. If this was set up on a block chain, it'd be no you would not able to refute it.And so I would suggest when you do, I don't quite understand how you'd have to report on these technologies. But I would suggest you, Andrew, like you should say, like. Most people will think of blockchain and crypto currencies being applied in financial services because that's kind of where it started. But the most transformational use cases of blockchain are in agriculture, food, luxury goods, farmers like Lifesciences. I mean, that stuffs the life science stuff is so important, so important because it's life and death. If people are taking a shitty drug that has come from Mexico instead of like New Jersey, they could die from that And it's, you know, it's I think. That is super exciting. I also think like another technology that's. I prefer to think more about like humanity's humanity and helping people live a better life. I think that connected devices. So like wellness. And it's not just like the watch you wear. It is the ability to do drug trials where it's a device that people consume. And then the drug research at the lab can see how that is working through the body and the cellular impact that the drug is having on the person. And you think about like the speed. So the reason they can create a vaccine in like a year versus 20 years for COVID is because they have these sort of technologies. If they didn't have that normally in the old days, a vaccination took 20 years to create like millions of people would die. And in a non COVID world like the use of those technologies allow people in Third World countries to get access to medical treatment that they ordinarily would have no access to. So I personally feel really passionate about technology and life sciences because I think it's going to help som many people.

[00:40:41] Ben Matthews
Yeah, that's fascinating.

[00:40:41] Samantha Gloede
I'm such a nerd

[00:40:46] Andrew Moloney
That was really good.

[00:40:47] Ben Matthews
Yeah. I have a different question if I have time for one more And so obviously, like long story short, the question is like are you able to talk about some of the worst days you've had in your role and the things that have gone wrong. Is that the thing that you're allowed to talk about?

[00:41:07] Samantha Gloede
Yeah, I can.

[00:41:09] Ben Matthews
I just want to Get the best of that, like the highs and the lows of the drug.

[00:41:13] Samantha Gloede
I definitely can. I can give you guys some big examples, too. Sorry, I lived in New York on September 11th And there's so many things about that day. So we I was working in downtown New York City. I'm looking out there right now. And I was working on the audit for Citigroup. So one of the biggest banks in the world. And we also had a team that worked for Deutsche Bank, which is big German bank.And why back then? Gosh, it was like 20, 20 years ago.

[00:41:45] Helen Nowlan
I cant believe how long ago it was

[00:41:45] Samantha Gloede
So About 10 years ago. Crazy. So at the time, we didn't have proper backup So we would just once every month drop a copy of our server off to the other office. Didn't think anything of it. Both buildings collapsed on that day and we were nine months into a twelve month audit. We lost every hard copy because the building burtn down. We lost our soft copies. So we had somehow we were able to sign off the audit that year. God knows how, but like, that was a pretty big scenario. And I remember at the time, like one of the big areas that we focus on is around, like business continuity and resilience. And that was. And it's sort of I guess we're in a similar situation now in a way, when such a massive disaster happens It doesn't really matter what backup or additional processes you have in place. If you don;t have the people there to do work and the technology to support it, you can't operate. And so back then, it was like limited to this geographical location in New York City. But now you're looking at a pandemic that's impacting every single country in the world and every single person. So it doesn't matter whether you are an executive that operates in like the most senior level or you're the person in the back office who is plugging in like the server room or you are the person doing the deliveries or you're the person taking the phone orders or whatever the hell it is that you do. Like every single person has been impacted. So. It's been Exciting in a way, to see how we can help our clients, but also incredibly stressful because you realize, like people are surviving right now and they can't afford to spend money on things. So they cutting a lot of the nice to haves and just spending on the absolute must haves. So that's been a huge impact to our business. I had another example also in New York where I was working for a telecommunications company that provided all of the technology for JFK Airport. And I remember I was sitting there, I was young at the time and. Not like I I was a manager, but like I was a new manager and I was really nervous and it was like when the first reports I was presenting on my own and there were a lot of findings, like we basically they had no backup. And I remember, like, they were arguing with me, it was like these big older men and they were like, you don;t know what you are talking about this never going to be this issue. And literally in the middle, I'd said to them, like, either way, if you lost all connectivity, how would all of the airplanes continue to operate at JFK? And he said that would never happen. And then let's literally within five minutes, there was this massive blackout and all of New York, all of the whole state, was like blacked out and they lost every connection. JFK was completely grounded. So it was like the worst stressful situation. But it was kind of like the best time in my career because I was like But then also, like, we've had security incidents that are really stressful where, you know, we were involved in trying to anticipate scenarios and hackers got in. That's not fun. We do really big projects for banks. They have a big regulation called Know Your Customer. And it's basically started around like the global financial crisis in 2008, where people were like fraudulently getting mortgages and loans and all this stuff or entering into like financial agreements that they couldn't sustain. And so now the banks have this massive regulatory requirement to go through this whole routine with every single customer, whether it's the person that gets a credit card to the like billionaire who's trading stocks with them And the cost of that is really significant. So, like we have a six hundred million dollar contract with a major bank to do that whole process with them for them And we had a big fuckup with our process. And it kind of wasn't working. And that was six hundred million dollars on the line. So I think that anything can really go wrong because technology can't you know, you're not God, you can't control everything. And I think that there is still an assumption that, like, if you're in technology, you know how to fix everything. You don't always know how to fix everything because anything can really go wrong. So, I we always tend to be Cautiously optimistic about things like this huge opportunity But we also very, very well aware that with technology supporting so much like so much can go wrong. And it can be pretty stressful to. As you guys are going through, like your degree, if ever you want advice on, like, companies to work for jobs to go for, like, Helen can put you in touch, I'm totally happy to answer any questions, because what I do, I work with so many different roles in technology so I can probably help figure out, like, if it's a good fit or not. I'm really happy to do that.

[00:47:23] Ben Matthews
Thank you so much

[00:47:25] Andrew Moloney
Youve been such a great help

END OF TRANSCRIPT