
**Speaker 1:**

This is a podcast by Lumina, the perfect space to innovate, collaborate, and grow in health, science, and tech.

**Rebecca Griffin** - Host:

Damien Seaton, welcome to Health Tech Talks.

**Damien Seaton** – Guest, Thank you.

**Rebecca Griffin** - Host:

Damien. You're the managing Director of Cyber Audit team, an independent provider of Information Security and Cybersecurity Specialist Services here on the Gold Coast. Over your 30-year career, you've worked across many areas from cybersecurity, Information Security and Data Protection to dark web threat intelligence, digital forensics and criminal psychology. And you were a senior detective in London's Metropolitan Police Specialist Crime Unit where you were responsible for investigating and prosecuting some of the UK's most complex and serious crime. What a career, Damien. So can we start with your work with the New Scotland Yard? What drew you into law enforcement?

**Damien Seaton** - Guest

I guess, I was in the, well first I was in the Royal Military Police, and so that had an element of investigations. Basically what they do is they investigate crimes relating to military personnel around the world. And I worked in an intelligence agency there and that really helped me understand that's what I wanted to do. It was a protection element of helping people and giving back. And I was actually then based in London for some time and during that time, I worked very closely with Metropolitan Police and it seemed like a natural progression at the end of my career where I'd thought seven to eight years was long enough, and I wanted to stay in London and not be posted overseas again.

Rebecca Griffin - Host:

And so that was then New Scotland Yard?

**Damien Seaton**- Guest

Yeah, London Metropolitan Police, New Scotland Yard. And I started off as a rookie, [inaudible 00:01:45], and then just progressed my career from there.

Rebecca Griffin - Host:

And a lot of the work you did was investigating complex crimes as a senior detective, and a lot of that was in cyber crime, organized crime and complex financial fraud. How has cyber crime changed over the past, say, 20 years?


**Damien Seaton**- Guest

Well, that's a good question. And back when I was in, which is in the early nineties, it was actually computer crime. So cyber wasn't a word. The internet was very much in its infancy for the general members of public, but there were still computer crime happening then. So we're talking basic fraud, deception, and people would use their computers to actually do that, whether it's sending emails to people. So emails existed, but the way that we now know the internet is very, very different. And so that's progressed over the last 30 years, I guess, because now it reaches so many people globally. Anybody can do it. It's not difficult.

And so cyber crime has changed because we've allowed technology into every aspect of our working lives and probably more concerning for some that we've allowed it into every part of our private lives, our home environment, and we refer to that as internet of things, IOT. So in your home, you might have a fridge that connects to the network or a doorbell or a baby monitor or a PlayStation or an Apple TV. And all those devices have pretty much zero security on it. And just over the last, probably, 10 years, more and more people have learned how to find vulnerabilities in these systems and exploit them.

**Rebecca Griffin** - Host:

What interests you in cyber crime and cybersecurity and led to your long and successful career in this space?

**Damien Seaton**- Guest

Well, I guess, that it's something that whether we look at it now and cyber is very broad, so it encompasses a lot of different areas. For me, it's about helping, still helping businesses, whether I was a police officer or was in the military. Even now it's about helping businesses and individuals to understand how they can protect themselves, their families, their business, as well as conform to regulatory compliance, whether it's ASIC, APRA, that sort of stuff. And understand that, and it's probably one of the biggest issues that every business in Australia suffers is they have a lack of understanding, but it's very broad, it's very exciting. Every day is different, never the same issues are faced on the same day, but very similar things that happen. But it's just an exciting industry and career to have.

**Rebecca Griffin** - Host:

Are there new things popping up all the time that you haven't experienced in the past?

**Damien Seaton** - Guest

Yeah, absolutely. I think as technology advances, so we see a lot of common things that are common every day, like phishing emails where somebody sends an email out without your name, it's just hi or dear customer. So it's just think throwing a phishing net out there and hopefully we catch some phish that's very common and you see that all the time. But what we see is what we call threat actors or the criminals using various tactics, techniques and procedures, TTPs, and they change based on the advances in technology.

So think about a burglar that wants to burglar your home and you put a front door with a lock on it while they might go around the back of the house, and then you put a lock on a door and they get in through a

side window. So then you put side windows on and locks, and that's what we call defense in depth. So your own house now has doors, windows, window bars, cameras, lights, maybe a dog, maybe a wall. These are ways that you defend your house. And so we're trying to keep up with the criminals because they're financially motivated to take our data, our information, or our finances.

**Rebecca Griffin** - Host:

So, they're finding these back doors, these side windows. That's a great analogy and helps to really understand that cyber space, I guess.

**Damien Seaton** - Guest

Yeah.

**Rebecca Griffin** - Host:

So as you mentioned, you work with businesses supporting them to ensure that they have adequate cybersecurity. So just for those of us who don't know, can you explain what cybersecurity is?

**Damien Seaton** - Guest

Cybersecurity is many things, but at its core, it's really about protecting anything that connects to a network or the internet. So if you think of what we call endpoints or devices, your mobile phone, your laptop, your tablet, your servers, your web applications, your clouds, anything like that that's connected is vulnerable. And so cybersecurity is tasked with trying to protect that. Fundamentally, that's the problems we said earlier on with cyber securities. It causes individuals and businesses to think more about technology and then they think that's it's problem. But everything is designed at the moment or used by a human, and that's the weakest link in everything.

The cybersecurity also has to cover, not just the technology side of things. It also has to teach the humans how to use that technology safely while showing them how easy it is to deceive them or to socially engineer them. So that's getting them to do something that if they knew I was a criminal, they wouldn't help me or talk to me. But if I can pretend to be somebody that they might trust or gain their trust, then I can get them to do things for me or tell me things that otherwise they wouldn't do. But cyber can cover a lot of things, but really fundamentally, it's about protecting the information, the IP of a business, the website of a business, anything that's connected to the internet.

**Rebecca Griffin** - Host:

Are businesses becoming more aware of the need for less protection?

**Damien Seaton** - Guest

I think they are now. We've been doing this for seven years at this particular business. And I think really what happened late last year was the number of data breaches that were significant and particular the ones that really hit the headlines unfortunately, which was the Optus data breach and the Medibank data breaches. And that's really thrust this to the forefront of most directors and board's minds providing that they're not then bamboozled or just told by their IT, "Don't worry. We've taken care of


this" and this is a fundamental shift. It needs to have a changing culture. And it's just education. It's not saying that IT can't do this and shouldn't do this, but IT are tasked with running the day-to-day operations of the business to ensure that the technology is working. It's there to make sure that the software is licensed correctly and it's working.

And now we're asking our IT colleagues to also take on this little thing called cybersecurity or information security as well. And often, they're not trained in security, they don't come from a security background or security engineer background or a cybersecurity background. But most businesses are saying, "Well, with the same budget that you've already got, can you please also do this little thing called cyber? And this is just education." So it's educating the boards and the directors that you should actually really separate the budget out because IT have got, some might a good budget, but often they're quite small and they're unbudgeted. And then we're asking them to do a lot more.

**Rebecca Griffin** - Host:

Can you tell me about the current cybersecurity landscape in Australia in the Gold Coast?

**Damien Seaton** - Guest

Well, it would be Australia. So I don't think that the criminals particularly target individual or different areas of Australia. However, with a caveat there, obviously Canberra because there are very large organizations there. But also it's where our government sits. So that does get targeted a little bit more, but that would be more what we call state sponsored. So if you think of the China, North Korea, Russia, Syria, that sort of areas, there's state sponsored, so that's the government sponsoring criminality against a particular country. But they're also looking for things like intellectual property. They're looking at universities that are big target in Australia because we've got some of the best universities in the world and out of those universities, there's a lot of IP that comes and if they can take that information as opposed to developing it themselves, that's very simple and it's one of the things that most criminals look to adopt is the path to least resistance.

If they can get to their end goal much quicker, well there's a better return on their investment. So the landscape in Australia, it's still, we're seeing probably the number one attack vector is phishing or spear phishing where they do use some details. It's very easy for a criminal these days to gain enough information of most individuals online, whether that be through LinkedIn or one of the other social media platforms or even just in the news in general. And then have just a little bit about yourself, a little bit information, and they can use that then to their advantage to deceive you. But we're also seeing ransomware. Now in 2018, ransomware really had a dive. It almost didn't become extinct, but because businesses were ensuring they had the right backups, that they had relatively okay security in place, it became more difficult. But what all the criminals did then is they changed and they pivoted and they went straight after backups.

And so they were able to shut businesses down and then extort them for huge amounts of money into the millions. But what we're seeing here now is a lot more of the social engineering deceiving people. We're seeing a lot more business email compromise, which is where somebody will compromise your email. Maybe it's a senior person in the business, the CFO, the CIO, the CEO, and then they will send emails out to anybody in their collective inbox pretending to be that person and asking for something, whether it's for as crazy as iTunes cards, whether it's to do something on their behalf, whether it's to


provide them with some information or whether it's to change, if it's the CFO to change the BSB and account number for a new invoice. There are so many different tactics, but a lot of it uses, it starts with the same thing and it will be a phishing email, a phone call, or a loss of credentials, and that's username password because lots of people still use the same password across multiple sites.

**Rebecca Griffin** - Host:

You mentioned before about the large corporations in Australia last year that we saw having cyber attacks. Do you think we can expect to see more of this?

**Damien Seaton** - Guest

Well, we are seeing more, and even at that time there was probably another half a dozen that flew under the radar where we had Woolworths, there was Telstra, there's a few others as well that just made the headlines a little bit. But because the Medibank and the Optus were receiving so much attention, particularly from the government as well, but we're not just seeing the big businesses. The big businesses, they can probably weather a lot of this storm. They probably have the financial capability to work through these incidents. But what we're not seeing and what we're not hearing about are the smaller businesses in Australia. And Australia is made up of many, many tens of thousands of small businesses. And it's those ones that suffer. And those are the ones that we want to try and help where they don't have the resources, they don't have the understanding.

They have an IT provider or an IT manager that says, "Don't worry, everything's fine. We've got this covered." And they may have a few software solutions in place and they're the ones that are most exposed because they're busy trying to keep their business running. And it's very difficult for most people to, when you start a business and you're in that first seven years period, every cent and every dollar counts. And those are the ones that probably most at risk. Those are the ones that if they do have a breach, they don't report it because there's going to be brand and reputation damage to them. So we're not hearing of those ones, unfortunately.

**Speaker 1**:

You are listening to Health Tech Talks, a podcast series delivered by Lumina. To find out more about Lumina, visit the website, luminagoldcoast.com.au and sign up today to receive your Lumina opportunities pack.

**Rebecca Griffin** - Host:

What do you think are the opportunities and challenges across cybersecurity in Australia?

**Damien Seaton** - Guest

Well, I think the number one opportunities is education. And I would really encourage the government at all levels, state, federal, and local to start educating on this because just teaching people things like don't click on links, it doesn't work. We have to click on links in our day-to-day lives. Links are sent to us internally, links are sent to us externally, and that's just an archaic way of trying to deal with it. So I think the first opportunity is education, to help people understand what it is, what cybersecurity is, what it

isn't. It's not an IT problem or a technology problem, it's a whole of business risk and that we each have an important part to play in it. I think the other opportunities are we are now have think it's around 30,000 person shortage in cybersecurity. So we lost a lot of people when we closed down for the borders or when we had COVID, so we lost a lot of the international people that were working here.

We've also had a massive increase. So the government are increasing their requirements, and we've got a very small pool of dedicated cybersecurity specialists. So what ends up happening is we government might pinch some of our staff or pinch in from each other. And so there's not enough people to be doing this. So likes of Griffith Uni where we are, we've partnered with Griffith and the Busy Group to look at educating the students coming out their IT courses who have an interest in cyber, but they're unemployable to go and work in a cybersecurity company because they don't have the cybersecurity skills or experience. And you often say, come back to me in two years when you've got the experience. Well, where did they go to get that experience? So recognizing we've got a massive shortage, that's what we're going to try and help with, is give them the real world experience of working in a cybersecurity company, an organization, and give them that training. And I think that's one of the biggest opportunities is to encourage more diversity, get people working in this industry because it's a very exciting industry and it's ever-growing.

**Rebecca Griffin** - Host:

You're the founder of cyber audit team or CAT, what does CAT do?

**Damien Seaton** - Guest

When we first started some seven years ago, it was really to help businesses identify the risks or the gaps in their organization. And we use a framework, the ISO framework of 27001, and that was a framework that we started using. So at least we could give a company an idea of where their gaps were and what they could do to mitigate and remediate those gaps with a very detailed roadmap. Did have a technology roadmap for the technology people, but even at director's level, they could understand what their risk were, decide how they wanted to mitigate that. Very quickly, companies were saying, "Well, this is great, but who's actually... who can I go to?" Seven years ago there wasn't lots of companies doing this. And so very quickly we accepted the challenge and grew the business to then provide additional services, whether that would be training staff, because again, you can't just say, "Well, we've told everybody to not click on links.

Do they know about social engineering? Do they know about all the tactics that you use? Can they spot phishing emails? How do they report them? What is the culture in the organization? Is it from top down? So we devised the training element of the business and then we also devised another area to identify, because any attack, there are often many indicators of compromise. So think again, like someone trying to break in, the outdoor light might go on, the dog might be barking, a window might smash. Yeah, nobody's broken into the building yet, but these are all indicators now, if somebody was watching that building, they'd be able to investigate it. So we call that managed detection and response.

So that's security analysts looking at a business and looking at all their digital environments and seeing anything unusual that's happening. And if there's something unusual, they want to look at it and think, is that normal behavior? Can I clarify that that person should be logging in at this time, or do I need to investigate it? So that's a managed detection response that sits within our security operation center, or


SOC. And then we've grown then to provide penetration testing, vulnerability testing. Each time the customer wants something, a managed service, we analyze whether or not that's going to be something within our wheelhouse that we can provide or whether we introduce them to one of our partners, but we're an end-to-end solution provider that partners with our customers to provide them a holistic cybersecurity solution.

**Rebecca Griffin** - Host:

How are you different to other cyber audit businesses?

**Damien Seaton** - Guest

Well, I'm not sure about cyber audit. It was a name that we came up with seven years ago, and we will be rebranding now as the business has grown. But other cybersecurity companies, if we think about those, I think in Australia they're all really good. I think a lot of our competitors, we try to partner with them so that we can understand that not all of us, even if we all work together, could still sort this out. So unlike a lot of other businesses, whilst there is a lot of competition, I think it's really important that we collectively come together to assist Australian businesses, to assist universities and governments to understand this and use our collective knowledge. And I think that most of them that are out there are really good at what they do. So I wouldn't like to say that we're better than any of those. But what we do personally is we do partner with our businesses, we embed our staff with the businesses. We try to understand their specific industry and their specific challenges as opposed to one size fits all.

**Rebecca Griffin** - Host:

Is there something at a very minimum that businesses should do to protect their information? Or does it depend what sort of business they do?

**Damien Seaton** - Guest

A good question, and look, it is based on every individual business. What are they protecting? Let's think of a coffee shop. Well, most people would say, "Well, the coffee shop doesn't need to do anything." But if they're offering a loyalty program, then that might be their crown jewels. So what we try to do first is understand what are our assets? What are our crown jewels? What are we looking to protect? What would really damage the business? If a cyber attack, a distributed denial of service, somebody took our website down or we lost information, customers information, what would do is the most damage?

Once we understand that, what are we trying to protect? It's easier to work backwards to then be able to offer what's the best advice. But I mean, if we look at what's the most common, it's human error. So education and awareness is where it has to start at the board level or at the business owner level, director level, because leadership starts at the top. And if us as leaders aren't doing what we say we should be doing and demonstrating how we do that, then our colleagues and our staff won't do the same.

**Rebecca Griffin** - Host:

Is education part of what you do for the businesses you work for?


**Damien Seaton** - Guest

Yeah, 100%. Education's probably one of the biggest things because once staff understand what the risk is, not just to the business but to them. So what we do as an educator is we will actually train because staff because staff have to do a lot of training. Think of health and safety training, fire training. If you're working in Brisbane or one of the big cities and you work in a high rise almost on a regular monthly basis, there's evacuation drills. Well, everyone knows that if there's a fire, I've got to get out of the building. But we do need drills on a regular basis. Very few companies are doing that in cyber. Well, I've told everyone don't click on links, but what about the phone calls? What about their home environment? Are we teaching them how to protect their families from common scams?

The hello mum scam? So there's many, many different scams that are out there. So what we try to do is educate the staff, how to protect themselves and their families, their moms and dads or their children first, once they understand those risks and how simple it is to put some very simple controls and mechanisms around to protect them via osmosis and that reverse psychology, they'll bring that same education into the business, and they'll help us find things in the organization that we may not have known, or that they've downloaded a piece of software that now they realize there's no multifactor authentication or it's insecure. They can become our greatest asset and our human firewall.

**Rebecca Griffin** - Host:

You are based here at Lumina, which is the Gold Coast's Health and Knowledge precinct. How has being here helped your business? And you've talked about collaboration, so I'm wondering if that's part of how it's helped you guys.

**Damien Seaton** - Guest

Yeah, definitely. Initially, I must admit, I was skeptical about coming into these types of establishments and in a cohort environment, but then if I think back to my master's degree and in that cohort, I learned more from my cohort than I really did off the course. So listening to other people, their points of view, and one of the things here was, I think, the cohort here, they put on a lot of the information evenings, they do a lot of the hubs, and we've got to know a lot of the other tenants, particularly secure stack upstairs with Paul McCarthy, and we've actually started working together. So his product is fantastic. It really suits a lot of our customers for vulnerability scanning. And so there was a synergy.

And I think that when you come to places like this, you know, could be around, have gravity, lunch, making a coffee, you're chatting, even just imparting some of our knowledge at no cost and just explaining what we do. It's more engaging. Definitely being someone like here is, it's more relaxed, but you get to meet so many different people, you get to hear about their businesses, and there's a lot of collaboration that definitely goes on. So a lot of opportunity.

**Rebecca Griffin** - Host:

There are a lot of healthcare organizations based here at Lumina. How important is cybersecurity in healthcare?


**Damien Seaton** - Guest

Healthcare are one of the biggest targets, and if you think about the information that they hold, like a financial institution or your accountant, they probably hold a lot more sensitive data. What people don't realize is how information can be used for nefarious purposes. So if we think about being able to get your health records, and if we look at the Medibank data breach, that information was enormous, that they took, 9.7 million people lost their information, both current customers and previous customers, and the type of information that criminals want. Often people think it's just their bank accounts and things like that, but I can change a bank account, I can change a password, I can change a credit card very, very quickly and easily.

I can't change my health details, I can't change my identity that easy. And criminals will use it in various ways. If I wanted to blackmail somebody who works in a business that I wanted to target and I wanted to blackmail them for just their username and password to their outlook or to the system, and I've got the health records that tell me about an STI or an abortion or something that's really, really personal and terrible to know and use that against them, for example, I could use it for medical fraud, insurance fraud.

There are so many ways that criminals will use this information and because of that as well, yeah, I can also use it to deceive someone and to think I'm a doctor or a physician because I've got this information about them. How would I know if I didn't have that information? And so there's many, many ways that criminals will seek to use this information, and that's why healthcare practitioners and software developers in the health environment need to understand that that information is highly unevaluable, but we don't know how that individual's going to use it, just knowing how they've used it in the past and how they use it moving forward.

So going back to police days, this is just very similar to what used to happen in fraud, deception, theft. It's exactly the same, but it's in an online environment that allows an [inaudible 00:24:48], basically the criminal to be hiding wherever they want. And almost impossible for law enforcement unless they really, really lacks the criminals to actually find them, locate them, and actually prosecute them.

**Rebecca Griffin** - Host:

People can be so vulnerable as well if they are unwell or as you say, it's very personal information. So that vulnerability as well is just a whole nother aspect to it, isn't it?

**Damien Seaton** - Guest

Well, that's what the criminals rely on. So they want to use, do you think about any scam that they use it's going to be preying on your vulnerability, on your emotions? It's going to prey on urgency, sometimes. I need you to do something quickly for me, a favor, or if you don't get this done by this time. So they're very good at using the psychology against us. Now, whilst it's scary for a lot of people, the great news is it's very, very simple to protect yourself, and that just comes down to the education.

**Rebecca Griffin** - Host:

What other types of companies would you like to see co-locate here?


**Damien Seaton** - Guest

I think there's a really good diverse range of companies already, but I think that particularly the cohort here in South Pole has the opportunity to become a real leading tech hub, not just for Queensland, but for Australia. I remember years ago we talked about Silicon Valley and how great that was, and I think this could become a Silicon Beach. We're only five minutes from the beach, but this area has got a lot of opportunity. We've got the university, all these establishments popping up.

It's really great for businesses to be around each other so they can collaborate, they can talk, they can talk to founders, they can ask the right questions about starting a business. And I think that the majority of the businesses that we see here are all ready to give their time to help other startups. And I think I'd like to see, just more technology. This is where the industry is definitely advancing towards at a rapid rate, but more technology, more security companies. I really just think keep doing what they're doing, but attracting and showing what are the value propositions to come to somewhere like this and be exposed to other businesses.

**Rebecca Griffin** - Host:

Damien, it's been really fascinating speaking with you. Thank you.

**Damien Seaton** - Guest

Yeah, my pleasure. Thank you for having me.

**Speaker 1:**

To learn more about Lumina and how we work with Health Tech startups, visit luminagoldcoast.com.au. And don't forget to sign up to receive your Lumina opportunities pack today.