# ACCANect 2018

**Session 7: 11:05 – 11:25am**

**Keynote: Cyber security – Protecting what’s important**

**Presenter: Berin Lautenbach, Chief Information Security Officer Asia Pacific – Telstra**

**It has been another year of significant data breaches. Some of the big names having impact for Australian consumers include; Facebook, My Heritage and Page Up (clients include Kmart, RBA, Australia Post). In this session Berin Lautenbach will discuss the ongoing protections being used by organisations and how consumer data is being protected like never before.**

**11:25 – 11:30am Q&A**

JULIE McCROSSIN: Ladies and gentlemen, I'd like Berin Lautenbach

to begin moving towards the front of the room please. Berin will talk

to us about cybersecurity and protecting what is important, he's the

chief information security officer Asia Pacific for Telstra, and I think

among other things he'll talk about data breaches and also

protecting consumer data. Please welcome Berin Lautenbach.

BERIN LAUTENBACH: Love it. Thank you very much for having me.

I'll say up front, I don't like this sound of my own voice so this will

be relatively quick and then what I'm really interested with in

audience, a conversation. So I'll try and add a little bit of extra time

for questions. The Huge Bug, I haven't seen that video. That was an

absolute awesome video, but here's the thing. That comes from real

life.

JULIE McCROSSIN: I don't want anyone from Telstra to have a

technical problem Peter, are you able to help this? If necessary

island hand you the hand held. You can't just speak you're being

recorded for film.

BERIN LAUTENBACH: The...

JULIE McCROSSIN: I'll give him a mike.

BERIN LAUTENBACH: So the Hugger Bug, in case you think that's

just a joke, there was a set of articles around six months around a

doll in Germany that was actually recording through the eyes so

video cameras and listening to audio, uploading it to the Internet.

You can - if you put your evil hat on for a second you can just think

about all the implications that come from that. It's really scary and

it's kind of what I wanted to talk about and I'm going to talk about

three things fundamentally. What is a bad day look like in is

cybersecurity? I'll talk about how we think about it in Telstra just in

case there's some useful stuff there that other people might be able

to use but I want to talk about one of my favourite topics which is

hash tag team sport. How we need to work a little bit more

together. So what is a bad day in cybersecurity look like? I've been

doing this for 25 years and when I started I started in cybersecurity

by accident. I'm an IT geek who got thrown into a security career,

when I started I had one of the most academic jobs that exists in

IT. We would theorise about all the things that could happen. I

remember this - I worked in defence in one of the classified areas

and I had this conversation one day with my senior manager around

should we allow Internet email into our organisation? And my

answer was no, it's the invention of the devil. I went through and I

postulated because one of these things that happened but we

postulated me and a group of people, here are all the things that we

think could happen with email. We'll have data leakage, that's a big

deal in the defence organisation, but more importantly we'll have

anonymous emails, we'll have no-one attribute use of bullying, we'll

all all the things that we see today. All of that was a theoretical

conversation, what happened in the 20 years since it's all become

very, very real. I was at a bank when they first started putting

Internet banking on. We talked about I reckon there'll be some kind

of key board logging thing that will go out and will grab people's

pass words and everyone went it will never happen, science fiction.

Have a look at what happens today. And my thing here what is a

bad day in cybersecurity look like? We keep talking in my industry

about big data breaches. We talk about someone's lost 70 million

customer records, we talk about this big company that big company,

this big company, we very rarely wind that back to and so what did

that mean for those assistant million people? More and more my job

in my industry is about safety. It's about thinking and don't get me

wrong, data security incredibly important, but more and more what

can happen on a bad day isn't someone defrauded me of money and

I now need to go and deal with my banks, more and more it's about

there's someone looking through my webcam, or my car's being

interfered with while I'm doing 100km/h on a freeway. They're

really life impacts, to people and that's the big thing that the

cybersecurity industry has to real catch up with I think. It's not just

about data anymore, it's not just about big numbers and big

metrics, it's about peel's lives and what's going on. How do we think

about it, I'm going to whip through this, how do we think about it.

There's a conversation that happens inside Telstra and I won't say

this is unique to Telstra, I work a lot with people in my industry and

you can see similar kind of themes through the industry so there's a

conversation that happens at all layers in Telstra. The first is at a

beard level. There's a regular conversation with our board, it's quite

high level, we've developed a nice simple framework that we can

have an ongoing conversation around, and it talks about all the

things that you'd expect it to talk about, what's our context, what

are our controls, what are all the business processes we have to

embed this? Really important. But the bit that we've been really

driving for the last year or so and I think is actually key is how do

we turn security in a large enterprise into a shared accountability?

So there's a traditional model in security teams that's about

everyone looks to the security team - remember atlas Greek

mythology the guy who held the world on his shoulders, if you look

at his physique, I'm not too good at holding words on my my

shoulders, everyone looks at the security team and says they'll

make the problem go away. They'll solve it for me. In this world,

with the complexity of connectivity with the number of things that

we're doing, you need all parts of the organisation thinking about

security. So if I'm a developer of a webcam in the organisation I

need to be thinking about what are the implications when I put this

out into the public? What could go wrong? If I think about what

could go wrong what will I do about it? There's one trick in security,

it's a really simple game. If you think about it before it happens,

before you have put your product out, you can generally deal with

it. I'm not telling you won't get compromised, anyone who says

you'll never get compromise has rocks in their head, it will happen

and you need to plan for it but part of sit thinking about what it

could be and what could happen and plan for it. So we're embedding

people in development team, security championships program,

we're embedding, we an evangelist program as we're, we're fuelling

all the people passionate about it and there's a lot of these days

who really care about this so we're finding them all through the

organisation and helping them get a message out to everyone,

we're developing technical expertise in everywhere we can because

we're trying to get that culture of security right through the

organisation and I would posit if you want to do security well it's a

cultural things inside your organisation, you really need to think

about it as a key item. Then of course we do all the normal things

that you'd expect to us do, we do all the testing, we do the dry run

of something going wrong, pen testing ethical hacking, all the rest

of it but I come back to the core thing that I'm really driving at the

moment is how do I get a culture out there? So the last thing I'll

talk about, and then I'm going to open to questions and we can talk

about whatever people want to talk about, hash tag team sport. Ten

years ago, it was possible and I've been running security teams for

a while so this is how we used to do it. I used to sit inside my

organisation with a walled fortress, around my organisation, I used

to bring in all the tools and technologies that I needed, all the

people processes everything I needed and I would run security from

inside the organisation and I was fine. We had very much this

perimeter model, as long as I lock it down all will be good. In

today's world, not so true. We're all so interconnected that we've

got to start working with each other. So you'll see in the security

community all the silos of major organisation and some of the

middle and lower tiers as well get together and talk about how are

we helping each other? Some of that is the traditional stuff. How do

we share things going wrong, what are we seeing from attacks and

things like that? But some of it is much more about there was a

vulnerability recently in a particular package, that's relatively

complex to look at and solve, how do we bring some of the brains

around the various organisations together to solve that vulnerability,

to work out what to do with it? Because it's not a competitive issue,

if organisation X gets hacked, that's not good for me or any of us.

We want confidence in the overall system so us helping each other

getting that right is actually key I think to solving some of the

security problems. I go one step further, I keep hearing people tell

me we have a shortage of cybersecurity people. You don't want

more like me. What you really want is cybersecurity embedded in

the rest of our community, people thinking about it, thinking about

what matters to them, I've been having some wonderful

conversations lately, I just had one in morning tea, with people who

aren't IT security geeks, they're more community than that, they're

starting to think from a community aspect of what matters to me in

cyber. You don't want technical security people defining what's

good, you want the community defining what is good and then your

technical security people working out how to implement. Hash tag

team sport. That's really - that's a really important part to it and I

think if we do that, one of the things we'll start to see is if we start

treating security like a safety issue, then a whole bunch of things in

our community start to kick in, we're quite good at a community

level around safety, so look at things like - I've got four kids - we

had a baby cot back when they were younger and it had an

Australian standard logo on it but I had a level of confidence on it

that if there was something wrong with that cot there was a process

that would be followed by ACCC that would recall that cot or made

sure it was made good in some way, I would be notified of a safety

issue. I like the idea of taking some of these tools and techniques

that we already have in our bag and bringing them into the

cyberspace around treat it like a safety issue. And that forces people

like me as I'm building these systems to think about how will I deal

with it? Will I will able to patch the device? Remotely so that's quick

fix or will it have to be recalled? Anyway, hash tag team sport, all of

news there working together. It's incredibly important, I'll stop there

and open for questions.

JULIE McCROSSIN: Thank you very much. Would you give Berin a

round of applause. (APPLAUSE)

JULIE McCROSSIN: My mike's not on darl. If you could run down

with another one, in the interim I will raise my voice but I need

another mike. I want you to be able to answer questions. This is just

before we worry about the microphone, do we have a picture of

someone you can put up there? Have we got a picture of the

German doll. Cayla. I'll get you to use the lectern if you wouldn't

mind, I'm sorry. Can you just explain Cayla again because now we

can physically see her?

BERIN LAUTENBACH: I can't remember the exact time frame, it was

about six months ago, and I found out about it through some

concerned police people. And it's a doll and it's like a lot of these

things, it's a nice - someone's come up with a good idea. What do

they say the road to hell is paved with good intentions? There's this

nice doll that can listen to what the child is saying, upload it, can

see what the doll is seeing, upload it, put it in the Cloud

infrastructure and then respond to it. And you look at that from a

surveillance or more evil perspective, there's all sorts of bad things

that can happen with this. This is actually core to my theme, if you

think about this stuff before you put the product out, there's actually

things you can do, maybe there's parental controls, maybe there's

strict lockdown of who can see the data, maybe that's only uploaded

to a local PC and that's the only place it can go, there are things

that can with be done but we as almost a community need to be

starting to think about this kind of thing.

JULIE McCROSSIN: And communicating with consumer, Cayla looks

anyone. I could buy her for my grand-daughter at the drop of a hat.

This was obviously a huge paedophilea market on the Internet and

the Caylas of the world are designed for it. It's an issue of concern.

Questions or comments for our man from Telstra?

>> I'm from Internet Australia. First I'm surprised that comes from

Germany because Germany's got an incentive of any country to

privacy but when you say shared responsibility, it means there has

to be a sharing of knowledge, of awareness of how do you actually

get the responsibility and the knowledge of that out into the

community so that we can share it?

BERIN LAUTENBACH: It's actually - there's a couple of layers to this.

Generally when I talk about shared accountability, I think about it

inside Telstra and we have a whole program that's going on around

educating parts of our organisation, that almost become leaders in

their part right so I can't train everyone in everything but if I can

find key people in shares parts of the organisation then I can do that

but more broader community issue, I don't want people to become

educated the way I am. I don't need people to understand what

triple Des look like or how to authenticate or any of those things. I

want people to understand - and by the way I don't have a good

answer to this - I just know we need to be thinking about and I

suspect it won't be an IT geek who will come up with the right

answer to this frankly but I know we need to be thinking of this in

the same way, I brought up my kids knowing if you're in the house

on your own make sure the front door is locked, make sure the

windows are locked, there's some basic, we don't even think about

it as a community, we just bake this in when talking to our kids, and

we need to start thinking about this like that. We need to start

setting expectations so take that doll. As a community I don't

expect people to know what good looks like for that doll, but I do

expect a level of that's not good and I'm not comfortable wit and

you need to be taking that back. And looking at it. It's almost

accelerating the social expectations, I think that's what I'd like to

see us really think about. It's not a great answer to your question

because I don't have a great answer to your question, I just know

that we all need to be thinking about it and working on it.

JULIE McCROSSIN: We have time for two more quick questions. If I

could go for quick question and quick comment.

>> Two factor authentication seems like Google and Apple have put

a lot of security on telcos, is that something that worked with you

on, a lot of people place a lot of private information behind two

factor authentication?

BERIN LAUTENBACH: A couple of different layers to that. There is a

level of two factor that relies on SMS and that relies on the telcos

but you take it up a level and there are two factor authentication

methods out there that have no reliance on a telco or an

intermediary all at all and you'll see Apple in particular uses their

own devices now for two factor authentication. I really like that

model, I've got a new - you see it when you put a new device on

your account, it goes on and then all your other devices, quite eerie

if you have lot of devices but all the others in the house go ping,

there's something here, that's really flies because it keeps it in that

ecosystem. You have got it very controlled in your own ecosystem.

Relying on the telcos and SMS it's a good first step but not the final

step because you should never - you shouldn't have to rely on a

third party for this stuff.

JULIE McCROSSIN: Give us a sense of what the final step is?

BERIN LAUTENBACH: It is that piece of I've got this device here I

trust, I've got a very secure way of delivering a message to that

device, which is all done inside Apple's ecosystem to use them as an

example, I don't have to rely on anything else, it's all encripted,

controlled, authenticated, I can do it in any country in the world on

any telco in the world, I don't have to rely on any other security

other than what's built in.

JULIE McCROSSIN: I have two people dying to that talk to you.

>> We need to reduce as many barriers as we can so people can

their own security. Why can't we say downloads of security updates

don't cost you anything as a download. In rural areas we don't have

the spare capacity. We had a 10 gigabyte down load last year. More

security online requires you to be sent a code on a phone. Over a

million people don't have mobile coverage in their house, I have to

drive 30 kilometres to get that code. We think to think outside of

CBDs we need to think will will your security method work in all of

Australia?

BERIN LAUTENBACH: Yes. I can't say much more than that other

than yes, right? But I lifted up a level one of the biggest barriers to

security is user interface, how difficult we make it to be secure. So

the more - and I kind of look at it as if I solve that I should be

partially solving some of the problem you're talking about as well, it

should be transparent, I shouldn't have to think about it too much,

it's why I like the Apple approach of it just pops up on those other

devices and just go, "Yeah."

JULIE McCROSSIN: The only man I've ever met who likes repetitive

pinging. So I need you to be quick because I have another woman

here. You didn't want to say anything more.

BERIN LAUTENBACH: That's pretty much it. I agree.

>> Another aspect on that. There may be a lot security but you

realise you're dealing with Apple Google or Facebook and they're

flagging all your details, what do you do about that?

BERIN LAUTENBACH: That's a whole other area and I wouldn't lump

those three companies together. This is the conversation we were

having at morning tea. We need to get - I'm going to mirror what

was said to me at morning tea - we need tote to get very clear with

how data is being used, that's not actually - it kind of is a signer

security and it isn't. It's not a technical how do I secure this data.

Again I come back to it's a society, what are we OK with and why?

We need to get very clear. I take those companies, I'll pull out Apple

again, I'm not actually an Apple afficionado.

JULIE McCROSSIN: If you don't work for them in the next five

years...

BERIN LAUTENBACH: One of the things, because I'm a programmer

in my part-time, it is actually really hard in an Apple app to just

access the microphone. You can't do it. It will always put up a

prompt when my app gets loaded on your phone and says that I

want to use the microphone, Apple forces the question to you to say

is it OK to use the microphone or this data or access this or do

whatever. I love that. I really love that because that's what I think

we need to have, it's informed consent. That's the core.

JULIE McCROSSIN: How do we build it into teenage boys? One more

question.

>> It's wonderful that technology in the future is growing very

rapidly. I'm just conscious that with technology is rapidly involving.

I hope that the cybersecurity doesn't do so at the expense of people

with disabilities who want access to that. I am a self-confessed pilot

many years ago, I tried to access the caption but thank god for

Netflix I do that now but I remember the international relay service

where we were using the phone call to contact people, a massive

technology evolution back then but as soon as the banks said,

"Hang on this is the third person calling we can't have this so" so

they shut it down. From the interest of security it's good intentions

but they didn't realise there's a specific market to come in. We were

talking about cybersecurity and thinking of it, what about your

people, consider those who would need to access it and not the

expense of that. Did you have that discussion?

BERIN LAUTENBACH: Yes. I have a saying inside the organisation. I

am the last person you want making decisions about how to interact

with a customer. Because I will - that's the way my head works, I go

down the path of what's the worst thing that can happen here and

I'll stop it all. One thing we always make sure we do is we have

representatives from all part of the business and that includes the

customer advocates who are kind of looking at that kind of thing

and then offsetting me. So coming in and going I understand your

security issue but you have now just impacted this part of the

community, here's how and why, now I can work with it and

overcome it. But that's the whole thing of diversity in the workplace,

making sure you have all the representations on a particular

problem set but you never want me making all the decisions for

you, bad idea.

JULIE McCROSSIN: Would you give Berin a warm round of applause.

If you could pop atlas on the screen. It was a mention of Atlas and

I'm trying desperately to keep classical knowledge alive. Do you

have atlas for me, Peter. Just in case, if you could just get out of the

way, that's called atlas, who is atlas?

BERIN LAUTENBACH: Was he a titan? His job was to hold the world

on his shoulder.

JULIE McCROSSIN: Fabulous image, a round of applause for the

classical world, still so relevant in the digital age and