EMBRACING TECH IN FINANCIAL SERVICES EPISODE: NAVIGATING THE SOPHISTICATED WORLD OF RISING RAMSOMWARE

TRANSCRIPT

Host: Tim Broome, Technology Advisory Practice Lead, Accenture Australia and New Zealand
Guests: Dave Powell, Managing Director, Security Lead for Financial Services, Accenture Australia and New Zealand, and Mark Sayer, Cyber Defense Lead, Accenture Security, Asia Pacific

Tim: Cyber-attacks of all types seem inevitable. Prevention techniques can only help so much, but the real answer seems to lie in how we respond. Join me and my guests, Dave Powell and Mark Sayer to hear what the experts are saying.

Presenter: Welcome to Embracing Technology in Financial Services, a podcast brought to you by Accenture. In this 16-part series, we will hear from experts to uncover the latest in technology and trends in financial services. Now, here's your host, Tim Broome.

Tim: Welcome everybody. We're going to return back to a previous topic this week. Cybercrime. Last time we spoke around malware, but there's an awful lot more for us to talk about and investigate further. So, joining me, we have managing director of security, Dave Powell.

Dave: Great to be back, Tim. Thanks for the invite. It seems like we hadn't touched anything

at our last podcast.

Tim: Yeah, I think we scratched the surface, but there's a lot of interest and people want to find out more. Dave and I are in Melbourne, but joining us from Sydney on the phone, we've got the AAPAC lead for cyber defense, Mark Sayer.

Mark: Hi Tim. Thanks for having me. It's great to be here.

Tim: Welcome. Thanks for taking the time to be with this. So what are the types of things that you're seeing, Dave?

Dave: Well, it's probably the biggest one is ransomware. We're seeing a lot of companies be affected by ransomware and there's several ways to get infected. We talked last week about malware, malicious software. Typically, that can come through in an email with an attachment or it could come by clicking a link, where you actually go to a website and download it. Another attack called, watering hole attack, where you would be tricked to go to a website where there was some malware residing, and then that malware would come down into your machine. Once that malware gets into your machine, then encrypts everything it can find and everything that your machine connects to. Then up pops a very nasty little note on your screen that says you have been ransomed. Please pay us a ransom to provide the key to unlock the encrypted documents.

Tim: Yeah. So I saw a recent statistic. This is on a piece of Accenture research ransomware is up 58% in Australia. Do you think that's as big as it really is or do you think there's even more than that out there?

Dave: I think it's definitely more than that. Most of this stuff goes unreported. The reason is, some companies are able to recover from a ransomware attack, because they have good backups. So, they're able to reproduce their documents that have been encrypted. But many companies don't have proper backups to their stuff. Or in fact criminals are getting very sophisticated in the way that they start to attack. So, they are waiting for your backup to be encrypted before they then pull the key and demand the ransom.

Tim: And are these real or is it a fake attack that tells you that it's real?

Dave: No, these are very real attacks and many industries and many organisations are being affected by this. Quite a number have gone out of business, because they have been unable to replicate their customer database or unable to replicate their financial systems and records and invoicing systems. So, it's a real concern and one that small and medium businesses don't really understand that they are vulnerable.

Tim: Okay. And Mark, how do we deal with that?

Mark: That's a fabulous question. It's one of the biggest challenges that we're facing really, especially if cyber criminals who've traditionally gone after internet banking and financial services. As banks are getting better, they're looking for other targets, softer targets to try and target for these cyber crime types of attacks.

Mark: But as Dave said, we're seeing more and more smaller businesses being hit. They're really ill prepared to deal with these kinds of attacks. But I think there are some basic things, especially when you're looking at, you know, crypto ransomware that Dave was just talking about. Making sure that organisations have got backups. But more importantly and the thing that a lot of people miss, is making sure you can recover from those backups. We do a lot of work in incident response. So, when businesses are hit by these types of attacks, we've got a team that can go in and help them deal with it.

Mark: And one of the most common things we find is that companies aren't prepared to actually recover their IT systems from backups. That I think is one of the biggest ones. Probably the second one is, actually the scenario planning. So, understanding what you would do if your core ERP system or your email system or some of your business-critical systems were unavailable, because they'd been hit by one of these crypto attacks. How would you actually go about responding and recovering your business?

Mark: There's a statistic that we keep track of, which is usually the amount of time it takes

businesses to actually engage after a specialist incident response service provider. And that's typically about five days. So a lot of organisations struggle on their own trying to resolve things for up to five days before they actually bring in some external help. So, I think being prepared and knowing what to do in that situation is definitely advantageous.

Tim: So, is ransomware, in this context, theft of your knowledge or theft of your ability to recover?

Mark: Yeah, it's really denial of access. So they're taking away the information so that your people can no longer access it. Then charging you a fee to get that access back.

Tim: So, is a theft of the information relevant to attack as well?

Dave: That certainly becomes the one of the next levels. So if we move on from ransomware, many countries and industries are now trying to steal intellectual capital. So the data is very valuable. For example, if you may want access to health records or you might want access to some new technology that has been developed by some American company. So, we're seeing cyber criminals in nation states go after that technology. To steal that data. To then get an advantage in any industrial context.

Tim: Yeah, okay.

Dave: In a nation state context, you know, some nations get more blame than others and there's some obvious ones we've heard of in recent times.

Tim: Yep.

Dave: But you know, some of our so called friendly nation states aren't that friendly when it comes to this type of data theft.

Tim: And well, Mark, if we pull it down to a financial services in Australia lens, how does this really land in this space?

Mark: Yeah, look, it's a tricky question. I think financial services are accustomed to the very traditional cybercrime. You know, the online banking fraud and the malware that targets customers and the fraudulent transactions. But I think a lot of the things that Dave's been talking about in terms of nation state threat actors, but also some of the other criminal elements that are looking at ways to monetise.

Mark: And at the end of the day, cyber criminals are looking for the easiest way to make a buck. Targeting internet banking now is getting harder. So, things like the crypto ransomware, extortion attacks, also stealing information. Healthcare records and financial transaction records and not just of interest to nation states, but they're very much interested to cyber criminals who want to do identity fraud and identity theft.

Mark: So, we see a lot of that sort of information that's been stolen from all kinds of organisations, including financial services organisations, being sold on the dark web for criminals to use for their extortion and criminal activities. I think it is definitely a threat to financial services and one that is easily overlooked in the shadow of traditional cybercrime.

Tim: And is the defense to this, is this the same as the other defense? It's keeping all your systems up to date. It's training individuals on how to spot behavior or do we do something different here?

Mark: Yeah, I think we are seeing a bit of a shift. If I look at the last 10 years that the push into sort of making companies more resilient to these types of attack has really been focused on trying to prevent cyber-attacks. So, traditional controls like having antivirus current that the malware that's trying to be installed as Dave explained before. Having firewalls that prevent people from the Internet to being able to access all of your internal systems. All these traditional controls are designed to prevent cyber-attacks.

Mark: But, if you look at the trends over the last few years, we're seeing the number of attacks increasing and also the impact of those attacks increasing. So, the industry's now looking at it and saying, 'Well, we need to keep trying to prevent these cyber-attacks, but we also need to start investing more of our resources into detecting and containing and dealing with the impact of these attacks."

Mark: One of the key metrics we track in cyber defense at Accenture, is what we call the meantime to detection. So, this is the sort of like the industry average time across the number of incidents that it takes organisations from the time the attackers first get a foothold to the time they're actually detected. And that's currently tracking about 196 days.

Tim: Wow.

Mark: Which is quite, quite phenomenal. And so this is one of the really alarming metrics that we're looking at. And saying, "Well actually this is because companies are really struggling to detect these threats." So, we're seeing companies now investing in advanced capabilities to hunt for these threats in their environment and to look for the telltale signs left by, not just cyber-criminal organisations, but also some advanced nation states who are also targeting its commercial entities. So we're seeing a big shift in that in towards more holistic cyber resilience.

Tim: Are we also seeing a shift from trying to purely protect? When I think from the conversations we've had and what you've mentioned, that is only partially successful too. Then, okay, if we accept that an attack is going to happen and you're not going to be able to block every attack, then what's the best way to respond?

Mark: Yeah, look, absolutely. I think right now we're tracking the time it takes to actually respond and contain. Once we've identified that there's been a breach, that's in the sort of 69 days. That again is, you're looking at more than two months to get that down. This is where it comes into and I talked before in the sort of crypto ransomware for small businesses.

Mark: It comes into how prepared organisations are to deal with these kinds of threats. Do they have relationships with third parties that can come in and support them in incident response? Whether it be bringing in the expertise they need or bringing the tools or just bringing the human power. We worked on a major incident response late last year that went on for three months. Running 24 by seven. Now even the largest banks in Australia do not have the capacity to run a 24 by seven incident response for three months.

Mark: So, being prepared and thinking ahead about what you need to do when you do have one of these incidents, has a major impact on reducing the impact to your organisation. I guess and the time it takes to get it under control.

Tim: I would have thought even the wear on individuals being in a 24 by seven response team for three months. It must be hard work.

Mark: Yeah, it's a long slog. And when we've seen those kinds of ... These don't happen every day. Like these are the worst sort of case scenarios. But, when we do see these incidents, we generally see multiple vendors. It's not just Accenture coming in to do this. We have a whole bunch of different vendors. It could be their infrastructure providers, their application providers, and it could also be some other security consulting firms that provide resources.

Mark: So, you know, coordinating all of those different resources. Getting them working towards the one mission. Keeping track of everything that's going on. But also, as you say correctly, managing that workforce to make sure that people can keep going and have the resilience to see that through, is quite important.

Dave: One thing I'd add to that, Mark is really, this stuff is really difficult to get rid of. One, to find and two, to get rid of. One of the most common attacks today is to get a foothold in your environment. And the first thing criminals do when they get a foothold is go sideways and put sleepers into your environment. So you might have 20, 30, 100 sleepers in your environment. So, if you happen to find one and fix it and shut it down and clean it up. Very quickly another one starts squawking and actually taking over from the first one.

Tim: So, when you say sleeper, can you just expand on that a little bit?

Dave: So, sleeper is a piece of software that is replicated. So, the criminal would get a foothold in the first machine as part of the attack. Then they would go looking to the rest of you around and say, "Well, where could we hide the same

software?" So, if the first one gets disabled, then we can use a second or the third or the fourth one. These things live in crazy places that you would never find. So, for example, on the printer spooler.

Tim: Right. Not where people tend to go looking.

Mark: One of the best examples I saw of this, just to illustrate how difficult it can be to get rid of these threats from your environments they're in. There was a bank, not in Australia, overseas who had been compromised. They'd cleaned up the compromise from the attack. Got them out. Three months later the same threat. Actors are back into the environment. And this went on for about nine to 12 months. Eventually they found out where the sleeper was, was a copy of notepad.exe and everyone would have used notepad on the Windows computer. Just a simple text editor.

Mark: But what the attackers had done is they'd changed the code in notepad to the exe, so that when somebody ran it, it would go off to the internet and download the malicious code and start it off again. So, literally what had to happen to re - infect this network was that the system administrator needed to log in and just open it up exe and it would reopen the back-end door and let the attackers back into the environment. Those sorts of things are really, really difficult to find.

Tim: So something like that happens. How do you prevent it from escalating?

Mark: So again, as Dave said, when you get that foothold in the organisation, the thing that the attackers are going to do next is they're going to start to move laterally. They're going to look for systems of interest. They're going to be grabbing usernames and passwords that they can use to authenticate. And you know, what we see and from our experience, this is the Achilles heel that the attack has have. Is the time it takes them to try and understand their target's environment. And this is the best opportunity we have to catch them.
Mark: So the trick is to try and put defenses in place. Put ... We call them trip wires or canaries in the coal mine. The indicators that we can deploy into our environment that are triggered specifically when attackers are doing these types of activities. One of the things we've been working on here at Accenture over the past 12 months is starting to really do a lot of research into the types of techniques that these advanced attackers are using. And the mitigations that we can put in place. So, that we're getting these little tripwires being triggered when they're moving around.

Mark: When we refer to this as our high-fidelity signal. So, making sure that we're getting the right telemetry from the IT environment. Telling us when there's the telltale signs that the attackers are in there.

Tim: So Dave, when that happens, do you react immediately or do you allow things to proceed for a period of time to watch what's going on and better understand? How do you react?

Dave: Yeah. And I think you're onto both of them, Tim. Either option is the right one depending on what's occurring and what you're about to lose. On some cases, if you've got key data that's being ex filtrated right now, more recently in some things like the Singapore health data breach, you want to stop it right now. Because you're losing.

Tim: Yeah, obviously.

Dave: But often, as Mark said, these criminals are in your environment for a long time, nearly 200 days. So, they're looking around. They're doing bits and pieces here and there. So, if they're just looking around, it's a good idea to be able to just track them. See what they're doing. See what they're after and trying to get some attribution. As in, who's behind it and why are they behind it? What are they after and why are they doing it?

Tim: Yeh look that's really interesting.

Dave: And then you can start to work with law enforcement around what you might do about that. That's been a tricky component of this. Getting the international community to all work together.

Tim: Right.

Dave: But, is getting better with Interpol now in

Singapore. The cybercrime has traditionally come out of Romania. But Romania is now starting to clean up their act. Because they are a low-cost environment trying to attract call centers. So, therefore they're trying to improve their reputation. So, now there's a lot better cooperation between the intelligence and law enforcement agencies.

Tim: Okay. Look, if we can jump a little bit. There's a phrase I want to find out about. Hacktivist activist. What is that?

Mark: These are what we refer to as the ideologically motivated. So, unlike cyber criminals that are trying to steal money and nation states that might be trying to steal information or disrupt. The hacktivists sometimes just do it for kicks. Sometimes they might have a political agenda, whether it be the environment or something along those lines. And they want to use hacking as a means of furthering their message. We saw a lot of this activity, back to sort of five to six years with organisations like Anonymous. They would run from time to time, things like Operation Australia. Where they would try to get all these Anonymous affiliated hacktivists to try and break down Australian banks and Australian government organisations. We also saw groups like LulzSec, which was just a bunch of young people causing a bit of trouble on the Internet because they could.

Mark: What has been interesting and tying into Dave's point, just before about law enforcement and the impact that law enforcement has on this cyber security landscape, we've really seen a drop-in hacktivist related activity. The thing that I think correlates well with that has been the law enforcement approach. A lot of the LulzSec and Anonymous hackers that were involved in some of the biggest ideologically motivated attacks some years ago. A lot of them ended up in jail. We've seen a real downturn in the number of those types of attacks that we've been seeing play out in the industry of late.

Tim: Mark, it's worth talking about beyond that a single motivated person now versus a hacktivist activist. Anyone that has a vendetta against you or your organisation can cause a lot of damage.

Mark: Look, absolutely. One of the trends, one of the alarming trends that we're seeing is that a lot of the techniques we've seen nation states develop, and you would have heard about Stuxnet. The malware that destroyed the uranium enrichment facility in Iran some years ago. We're seeing those kinds of capabilities now making their way, not just into tools that the criminals are using, but also into simple downloadable tools that any 15-year-old kid can get their hands on and start doing really advanced types of cyber-attacks.

Mark: There's a free software repository on the Internet called GitHub, where you can download all these different sort of open source tools. On there you'll find persistence, libraries and tools written in power shell that are designed to bypass all of the common security controls and anti-malware controls that literally is just, you download it, you point it at something and off you go.

Mark: So, the capability that's available to the hobby sort of hacker today is quite substantial in terms of what they can do and how easy it is to obtain those things. So we do see the lone wolf types of attacks, where it could be an employee who's disgruntled or a customer who's disgruntled or someone who takes umbrage at a particular company for a particular reason. But yeah, to Dave's point, we have seen that sort of downturn in those organised groups where they were sort of operating under a particular banner or brand.

Dave: And adding to that Mark, if all else fails and you still can't operate that software that's freely available on the Internet like GitHub, then you can certainly buy cybercrime as a service. And on the dark web you can actually locate people that will do this for you. And for something like $200 for the month, will cause a very nasty denial of service attack to a large major bank. A denial of service attack, meaning it targets an application. Meaning you might not be able to get to the internet banking for a week.

Tim: Which has a pretty significant financial impact on a bank.

Dave: Exactly.

Tim: Obviously a reputational impact that goes probably even worse.

Dave: But, even critical infrastructure. I mean, if you can't get access to your banking for a week, then how you're going to pay your staff? How you're going to have any cash or credit? From a bank, there's a .... not just the money side of it, there's a liability side to it all as well as reputation side.

Tim: So what would you do about that?

Dave: Well, these things we really can't prevent these attacks occurring. It really comes back to really your two-pronged approach. You need a compliance slash governance approach. You still have to patch your systems. You still have to get your user access right. Has the right people got the right access to the systems? You have to do all of that.

Dave: But really, as Mark would talk before, turning the focus away from the compliance prevent side, which doesn't work totally anymore, to the detection response side to be ahead of the game with what we call an intelligence led approach. So, the intelligence understand what's your industry? Who are the actors? What techniques are they using today?

Mark: I was just going to add to that. So when we think about, you know, as companies make that journey from really focusing on prevention towards more holistic cyber resilience, there's four key capabilities that we think about that are really intrinsic in building a good market leading cyber resilience capability.

Mark: When we talk about these in terms of knowing the threat. Being the threat. Detecting the threat. And eradicating the threat. So, knowing the threat is really understanding who are the attackers that are coming after you? You can find this out by talking to your peers in the industry. Other banks. Who have they been hit by? Reading media articles. There's lots of information to really well inform you about who is the adversary that's likely to come after you. And once you have a bit of an understanding about that, you can then start to research what are their tools and techniques like?

Mark: So, if you look at some of these AAPT groups, these nation state affiliated groups. Like say, AAP28. Every time they do an attack, they use the same kinds of tools and techniques. So if you understand that AAP28's coming after you, there's a lot you can do to prepare your environment to be able to detect and contain those types of attacks.

Mark: The second thing is about being the threat. And when we think about this, we're talking about taking a look at your organisation through the eyes of an attacker. And this is incredibly useful. We did an example, we had a government client, we were running some services, cyber defense services for in Australia. And we knew that there was another government organisation in another country that had been hit by these attackers. And we looked at the techniques and the tools that these attackers used, and we overlaid them on our clients, because they were in a very, very similar sort of industry.

Mark: And we looked at all the ways that attack would have unfolded in our client. And everything looked pretty good apart from one thing. We realised that the database, if they did a dump of all the data from the database, we wouldn't have done a very good job at detecting that.

Mark: So, we took that adversarial approach. Then started saying, "Well, what does it look like from the hacker's perspective?" And we realised that the hackers coming in, they don't know the structure of the data in the database. But our applications and our people, they know the structure. So, there's a series of commands that you run to learn the structure of that database. Things like show tables and show databases that our production people in our applications would never run. So we developed those custom detection rules to say, "If anyone runs these commands, send us this alert and let us know what's going on."

Mark: If we received that alert, we're 100% sure that we've got a problem. So, that's really taking that adversarial mindset and doing things like red teaming and penetration testing is a great way to get that view of your organisation from the outside.

Mark: Then the final two things that kind of work

together is really building up that detection capability to make sure you're getting really high-quality telemetry for your environment that's going to allow you to detect these attackers when they're moving laterally. Which is the weakest point they've got. Then obviously once you detect them, that you're prepared, you've got the tools, the people, the resources at hand to be able to eradicate and get those threats out of your environment as quickly as possible. So those are the four key elements we see as being intrinsically important in building that cyber resilience.

Tim: So Mark, I really appreciate that. We are coming towards the end of our time now. So that summary or that approach that you've given is really, really helpful. Dave, anything to add before we close?

Dave: No, only that the threat is getting worse. And if I can give any advice. It's understand your adversary. Because, you might think that you're not vulnerable and no one's after you, but what we've talked about today, including things like ransomware and intellectual capital, criminals may well be after you and you're not going to expect it. So be ready.

Tim: Okay, so that's great advice. I've really, really enjoyed this topic. It's complicated. I think there's an awful lot for us to learn, but it's just a thoroughly enjoyable conversation I've had with you. So for anybody listening, if you want to find out any more about this topic, please feel free to reach out to myself, Tim Broom, Dave Powell, or Mark Sayer. Find us on Linkedin and we'd love to continue the conversation.

Tim: Dave. Mark. Thank you very much.

Mark: Thanks. Pleasure.

Dave: Thanks for opportunity, Tim.

Presenter: You've been listening to Embracing Technology in Financial Services. You can hear the entire series on the Accenture Vision App by visiting accenture.com/embracingtech. For more information on all our podcasts, please visit accenture.com.

[End of recording.]