accenture

EMBRACING TECH IN FINANCIAL SERVICES EPISODE: DETECT AND PREVENT – RESPONDING TO CYBER ATTACKS

TRANSCRIPT

Host: Tim Broome, Technology Advisory Practice Lead, Financial Services, Accenture Australia and New Zealand Guest: Dave Powell, Managing Director, Security Lead for Financial Services, Accenture Australia and New Zealand, and Mark Leadbetter, Principal – Data Security and Privacy, Accenture Australia and New Zealand

Tim: Is cyber security more of a threat to business, or the individual? And is emerging technology making the job of protecting our information harder or easier? Join me today as I unpack this topic with two experts in the field.

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, our practice lead, Tim Broome.

Tim: Good day, everyone. We're out in the field again this week, and I'm delighted to be joined by Mark Leadbetter, a cyber specialist, and focusing on data.

Mark: That's right, yes. Morning, Tim.

Tim: Lovely to meet you. And Dave Powell. So, Dave, ex-CSO of NAB, 12 years there, and one of our senior cyber specialists.

Dave: Hi, Tim. Thanks for the invite.

Tim: It's lovely to speak to you both. And for me, this is a topic that I am very, very thin on the ground. So, I'm really looking forward to absorbing as much information as I can. And look, I know you're absolutely specialists in this area, so it's going to be great to have a conversation with you. Can we start off with what are the threats these days and, I guess, how are they emerging?

Dave: So, let me start with that one. They're moving rapidly, is the point of it. But let me start sort of with - there's really five main areas that we're sort of seeing. So, there's cyber crime, which started off with things like phishing, which is, "We're the bank. We're doing maintenance. Can you just give us your user ID and password?" Which many people did. Cyber criminals made a lot of money out of that. Then customers got quite aware of that. So, then criminals started creating fake sites. And they'd trick you to connect to a fake site. You'd put your user ID and password in, they would then switch you quickly back to the original site, you'd put it in again, you'd go, "Oh, that must have been a glitch," when actually they'd captured your user ID and password. Banks today are, in our research, still shutting down 100 sites every month in fake sites. So, it's still quite active and still quite effective.

Tim: So, how does a bank shut an external site down?

Dave: Monitor for activity. They have special techniques where they get on spam lists and they monitor for fake sites and have special equipment to be looking in the internet to find those fake sites. And as soon as they find them, they go through regulatory authorities and other CERT (Computer Emergency Response Teams), to get those sites shut down.

Tim: Okay.

Mark: And of course, the motive for those types of attacks is stealing the money, right? Stealing cash out of your account, targeting the end user, the customer of the internet banking system.

Dave: So, it sort of moved on from there and they got smarter because that didn't work as much. So, they then created what's called malware (malicious software). And they'd trick you to click a link or download an attachment or something like that. And of course, in that comes some nasty software. It sits on your PC, and then when you log onto internet banking, you have a front screen where you say, "Send $1,000 from A to B," it creates a back screen that says, "Send $10,000 from A to C."

Dave: When you hit the send button, the $10,000 in the back screen is what sent, and not the front screen. So, then we're seeing more and more of that. Of course, then SMS was invented as a second factor authentication, you know? And now, of course, the biggest problem is most customers are doing their banking on mobile devices. So, now you have the SMS and the banking app on the same device. So, we're seeing new types of malware from criminals that do things like put a fake application or screen right on top of the real application screen, banking application. When you put your credentials into that, you're putting it into the fake piece of software, and they harvest the credentials. They also do things like inject SMS stealers. So, when the bank sends an SMS to your mobile phone, the malware immediately captures it, sends it to the criminals, and then deletes it from your phone. So, now they have your user ID, your password, and the SMS, of which then they use to access your bank account.

Tim: So, Dave, that sounds as though the challenge or the target is the customer outside of the bank's controlled space. Is that really how it-

Dave: Absolutely, and it's a bit like Whack-A-Mole. Every time you shut one down and clean one up, another one appears. But banks have got very sophisticated now about detecting that malware and detecting whether you're compromised.

Dave: And it can be as simple as things like, "This date timestamp on your browser looks like it's from Russia," to much more sophisticated detection like understanding different JavaScript and other attributes within the session that's occurring between your browser and the bank.

Mark: So, of course in that space, the criminals are looking for the weakest link in the chain, right? So, rather than attacking the internet banking system - which is robust, secured, controls built into it - they're looking for the weakest link, which is the end point of where the consumer is using, to actually log onto that system.

Tim: Okay. So, the target isn't necessarily the bank or the insurance company, it's the customer at the end that's the target.

Mark: The motive is to steal money for those types of attacks, right? So, they look for the weakest link, and the way they're doing that is to try and steal the money out of the consumer's bank account and move it into their own account.

Dave: And, of course, that is changing, though. And, of course, more and more we're now seeing organisations themselves targeted. And so, we saw that with malware, one of them was recently called Carbanak. $80 million[1] was stolen from a Bangladeshi bank some years ago now where the Swift system was actually targeted to move the money. So, criminals worked out how to get inside an organisation, then worked their way to find access to the Swift system, injected fraudulent sessions, and were able to ex-filtrate money from the organisation.

Tim: Okay, and Mark, can we just poke a bit at who's actually accountable in this challenge? Because we've got the bank, and there's the customer. And obviously it sounds like the banks are doing what they can to protect the customer. What is it that the customers themselves should be doing to try and protect themselves?

Mark: So, that's the better practice around your home PC, making sure it's patched, making sure you've got anti-virus on there, and then from a good practice point of view, don't click the links in e-mails. If you get something that looks too good to be true in an e-mail, don't click the link. That's how the malwares generally typically downloaded onto the end user's PC.

Tim: I quite like that Accenture tests us internally. We get the odd e-mail, which is a fake phishing e-mail. And they can often be pretty compelling. There's a few traits that they'll always drop in as known ways to find a phishing e-mail, but it's a good way just to keep testing yourself is to, "I did click on that link," is the warning that you've just been caught. And I think it's a good way for us to just keep ourselves aware that this doesn't stop.

Mark: The challenge there, though, is - and that is correct - but the challenge there is that the e-mails look very real. It's not amateur with misspelled words. They'll use the real graphics and logos from the website. It'll look like a real e-mail. And then the other challenge I see for organisations is, internally, there's so many valid e-mails that are sent around with links in that we click.

Tim: Yep, absolutely.

Mark: So, it's spotting the ones that are fake is the challenge for people. And a lot of the time, people just aren't thinking, they're just reacting and clicking links.

Tim: Dave, what do we do about it?

Dave: Well, it's a journey and a whole set of processes that you need to follow. So, in the example I gave there is the customer has an obligation really in this to make sure that they have their PC up to date, they are selective in what they click, and as Mark said, if it's too good to be true, it's probably not true.

Tim: Probably is, yeah.

Dave: But criminals are getting very good at that, you know? "We're from Australia Post and we can't find you. Have you changed address? Click here to give us your new address." And

[1] https://www.bankinfosecurity.com/hackers-target-swift-using-banks-odinaff-malware-a-9451

who is not getting a parcel sent to them now? So, these things are getting quite sophisticated. But then, the banks are getting extremely good at detecting this type of activity as well. So, they are able to spot it. They monitor your activity. They're doing some very fancy things with data analytics to start monitoring.

Dave: I talked about some technical attributes before, things like using JavaScript in browsers and things like that. But also matching that then with "You just sent $10,000 to an international account you haven't used before." Oh, that looks funny, you know? And matching that with, "We just saw some JavaScript in your browser, that's really bad. It's likely that's ..." And they're very simple examples, but through that, the detection is getting very strong.

Tim: And I guess in almost any walk of life, there are guards put in place to protect behaviour, be that somebody flying and trying to land an aeroplane, or somebody trying to do a banking transaction. And it's often not the individual issue that you spot which stands out. There's a number of things that, together, when you have that data, you say, "Actually, all these individual pieces of information suggest something bad's going to happen." That's where we need to be better - really understanding data together, rather than just looking at individual triggers or suggestions something might happen.

Dave: And that's the new wave. Security data analytics is where it's all actually going to, using data lakes to collect all this information and running these sort of analytics over it to detect and predict some of the activity based on some stuff that's seen before and some stuff that's predicted in the future. And these algorithms are getting quite sophisticated now, where you can learn and predict what might be happening from what's happened in the past.

Tim: And Mark, I guess that when we've figured out whatever the algorithm is, some machine-learning algorithm which can predict a certain type of behaviour, the next thing is somebody will figure out how that algorithm works and produce something that tackles it in a different way.

Mark: So, the threats are ever evolving, right? And for years - so for the last 10 years - criminals have been finding new ways to break in, security teams have been finding new ways to protect against that. So, it really has been sort of the leapfrog approach. So, absolutely, yes.

Tim: So, is the cost of protecting an organisation increasing? I'm thinking from the perspective of: as technology's evolved, we have better, probably more automated ways to predict what's going on and lock challenges down. At the same side, that technology's enabling more, probably greater volume and a greater complexity of attack, to compete with. What's the trend? Is the cost going up or is it?

Dave: Absolutely, it's going up. And it's going up for many reasons. One is many organisations have got to catch up. They don't have the basic controls in place, and they've been caught short a little bit and not understood that many of the threats are relevant to them, because they think, "Well, why would anyone attack me?" Right? Banks, it's very obvious. Other companies, not so obvious.

Tim: Yeah, that makes sense.

Dave: The second thing is, the threats are changing rapidly. Just when you think you've actually fixed one threat, there's another 10 appear, and different ways to address it. And the third thing is, technology is changing rapidly at the same time. So, we're seeing new techniques, like moving to the cloud, which provides a whole different set of issues and controls that need to be provided. And we're using new techniques like agile software development techniques, and things called continuous delivery, which bring a whole new set of threats that then you have to start to mitigate.

Tim: Yep, absolutely. So, continuous delivery. I've recently done a podcast all around the world of DevOps and how that's emerging. And in fact, we actually touched on the DevSecOps term and how that all fits in. But we were really talking at it more from the lens of DevOps engineers and how they see security starting to come in. So, coming at it from the security side, what's your view on how security gets embedded in all of that?

Mark: I think that's a critical area for organisations. So, vulnerabilities within the applications are not a new concept. But the speed at which we're now developing new iterations, new versions of applications, it's becoming more and more important.

Mark: The challenge there, typically, has been: it's not a security person that has to do all the security work in there, right? DevSecOps isn't about just a security person, it's about how you educate your regular developers into good practices of secure development. Now, absolutely security need to be there, they need to be helping and supporting that. But at the end of the day, it's quality of code is what you're looking to produce.

Tim: Yeah, look. I think the security of the software that's being developed always seemed to be something that was put to the end of the delivery cycle. And for better or for worse, that would be one of the areas that gets squeezed because there's a release that has to go live, and performance and security all get a little bit squeezed. And I think it's critical and really a great idea that if we embed it in at the start and right the way through, it's far better than trying to solve it all at the end.

Dave: Embedding it into each of the scrums is where the industry is going there. So, make sure you pen test as you go. So, as your developers are writing code, it's sort of being checked by more automated systems. The penetration testing is occurring as you go, not right at the end. Many of these processes are being automated, so every time you jump up a new capability in AWS or Azure, it's not an individual doing it, it's a machine doing it, so you know it's consistent, reliable, the same every time. So, that's where we're seeing DevSecOps move.

Tim: But does that also push a requirement for the systems where software's being developed and being tested to be more production-like through earlier on in the delivery cycle so that the pen testing you're doing while you're developing is actually realistic against what will happen in production?

Mark: I mean, that's always been an ongoing challenge, right? How your environments - so, your pre-production environments - mirror your production environment, absolutely. And I think at a true code level, a true DevSecOps level though, the code is consistent across those environments. So, getting that code right and getting the code developed in secure ways up front is critical. Yeah.

Tim: Excellent. Look, can we jump a little bit to data and open banking, because obviously open banking is coming over the horizon pretty quickly at this point. And for me, I've looked at open banking as... the concern that I've had around it really is from the trust of data from the perspective of "is the data being used in the right way for the customer?"

Tim: I've not really looked at it from the lens of, "When this data is shared outside of the core bank or whatever organisation it might be, how is that data being contained and controlled from a security perspective?" Is that something that you're looking at having to deal with, think about?

Mark: Yes. I'll add one more into there actually, which is around being transparent around what data you are collecting when it's talking about your customers, particularly when you start getting to the mobile apps that can record data. But yeah, absolutely, I see it as an area of concern. And I think we need to see how open banking evolves to know how big that is. But absolutely, consumers now... the whole concept of open banking is putting the consumer in charge of their data, right? In control of their data. So, the concept then being you trust your bank. We know banks invest a lot in terms of cyber security. We know they've got controls and good frameworks to protect the data that they're storing. Now as a consumer, I have the ability to ask my bank to share my data with a third party. As a consumer, how do I know whether that third party has got the same level of controls that the bank would have? And likely at that whole framework around how do we know those third parties that the data is being exposed to or being opened up to will actually have the right controls to protect that data when they've got it?

Tim: And even as far as, does the regulations require them to have the same level of controls as the bank has?

Dave: No, they don't at all. But what many of the banks are doing now are really taking the initiative. So they're actually coming up with programs to assess those third parties to make sure that they've got some reasonable controls in place, and they can be confident that those controls are being maintained.

Dave: Now, that's quite expensive in the long term depending on the number of third parties that you're actually sharing data with. But it is something that the industry is starting to do. And banks are taking the initiative around that to start looking at those third parties. I do hope that one day we will see some sort of a third party accreditation type program where you can be accredited to whatever standard and then be comfortable that that standard is being adhered to in that organisation, instead of every financial services company that's sharing data then have to go and audit each of those individual providers.

Tim: Yeah, and I mean we're clearly moving into new territory here. And, I think, in many ways, the tech moves faster than the authorities are able to keep up with. And you can almost look in almost any field, in some ways big tech is driving what is the way to behave, rather than it being controlled by a central organisation. I think that might change in time, but whether it's a constant chase to try and catch up with what is right and what regulations we need to put in place, I still think it's possible we may never actually catch up. If we look at the rate of technology growth, it might be a constant catch up. And then, it's probably down to areas like the security part of an organisation to say, "Well, actually here's what ..." In the absence of any clear regulation on what can and can't be done, "Well, this is what we're going to do as our organisation, because this is what we want to stand behind."

Dave: Yeah, and I think we're seeing a lot more of that, which is good for the industry, but it's an expense that's invisible to the client and the consumer that's, in this case, wanting to share their data.

Tim: So, does open banking actually increase the number of ways for a bank to get attacked? Because if I look at... the more APIs I open up, the more I've opened up my organisation for an external to come in and pull information out. Is the tech secure enough in that space that we think, "Actually, no, that's fine? We shouldn't really worry too much about that," or, "No, no, this is another way to break into an organisation."

Mark: Well, it obviously is a new channel, a new avenue into an organisation. But I would say, from what I've seen, the banks have been pretty good at developing secure APIs and testing those APIs. So, I haven't seen it as a threat that's being exploited at the moment. And the focus has got to be developing secure APIs, and understanding the data that you are giving access to through those APIs, absolutely.

Dave: And identity becomes a big issue in that, right? You know, have you got the identity management right? And are you managing that identity? So, as companies come and go, are you deleting those identities and not giving criminals a chance to emulate those identities?

Tim: And how easy is it to actually emulate somebody else's identity?

Dave: In the case of malware, it's very easy, because in the example I gave when we first started the conversation this morning, when malware's installed on your machine, the malware sits and waits for you to log on for real. So, it doesn't matter what authentication you use, the malware will wait for you to log on for real, and then it will steal the session. So, if there is malware on the end point device that's accessing the data, then it's quite easily compromised. Other than that, there are different ways to break passwords. For example, particularly if you use easy passwords. And the crazy thing is you might think you're being smart in the password that you use, but the likelihood that many other humans have used that password is really high. And so, they have these things called rainbow tables that you can use tools like Mimikatz[2] to actually break these passwords and hashes to gain access to these

[2] https://www.bleepingcomputer.com/news/security/malware-creates-cryptominer-botnet-using-eternalblue-and-mimikatz/

systems.

Tim: But we have too many passwords in our lives. There is too many places where you need a password, and there needs to be an easier way to actually deal with that difficult problem I think we all have, because the reason people use a simple password is because they need so many of them that you need something you can remember, or you're endlessly doing the, "Yes, I've forgotten my password, please reset my password link." And the painful experience of resetting passwords.

Dave: And that's been something that's been recognised as an industry issue that isn't solved yet. But there are a few companies in Australia right now that are working on that problem. If I give you an example of how that might be solved - we don't really know it's you.

Dave: It's the first time we've seen you, we don't even recognise your face, it's the first time we've seen you. But what you might do is to say, "Well, we'll connect to the passport system and see if the passport system knows you." Yes, they said, "Yes, we know Tim," Tick. "Okay, well we can't just trust that. We might go to the driver's license system as well and we'll check that to see if- oh yeah, that's Tim. Yes," Tick. "And then we'll go to the electricity company and we'll check and see if it's Tim." And so, now you've got some sort of distributed form to say, "Yes, this is really highly likely that this is Tim." And so, that's where we're seeing the industry move to, so it's not just a standard user ID and password, it's like a consensus of identities to really prove it's you.

Tim: Is blockchain anywhere involved in this? This is a bit of a leap, I know. But as you were talking, I was just thinking, "Sounds like the types of places where blockchain might have a use case."

Dave: You're on to me. You're on to me. But yes, that is exactly one of the technologies that could be used, because remember, in that example I just used there, blockchain doesn't have to record anything about you, it just has to record in an unbreakable format. "Does the passport system think it's really Tim? Does the electricity company really think-" And therefore, you then have an authority to get back to the original requester to go, "Yes, all of these systems really say it's Tim. And yes, we can believe these systems because it's in blockchain, which we can trust."

Tim: And Mark, how about other forms of identification? So, we've got... that's a piece of information about Tim. What about who Tim is, or something that Tim knows? Who wants to go after that one?

Dave: Well, I think the primary requirement doesn't go away. So, for example, if you want to open a bank account in Australia, you've got a hundred point check. You've got to walk into a bank, you need these credentials.

Dave: You have to prove it's actually you. What did I try and get the other day? A copy of my birth certificate. Same sort of thing. I had to go through all sorts of identity stuff to prove it was sort of me. So, I think, in that context, that's not going to go away.

Dave: To actually start that original requirement, I think what we will start to see is some companies specialise in that, so you don't have to do that everywhere, does that make sense?

Tim: Yeah, absolutely.

Dave: So, you don't have to prove yourself at a bank. What we're starting to see, and I'm not in a position to name those companies that are working on that in Australia, but there are several companies working on that in Australia where you can go as a one stop shop, and with the intention that other organisations, including banks, would then connect to that organisation to know that it was really you.

Tim: Yeah, look, I was also thinking from the perspective of a password is something that I've decided, it's a piece of information that I've selected, and my address is something that can change. What about my fingerprint, my retina scan? Where do these bio ID come into it? And is that something that you do next to, as an addition, or is it a replacement?

Dave: So, remember where I start in this, if you get malware, the malware waits for you to log on for real. It doesn't matter whether you use thumb scan, iris scan, it waits for you to use that for

real, and then it steals the session. But it doesn't mean you don't do the other because you've still got to get into the system. So, yes, all of those things are better than a password. But those two are still electronically recorded things that can too be stolen. And when you start having thumb prints, you can only get it stolen twice before you can't reset it any more, you know? So, what we're seeing is a bit of a different approach to that. So, we're starting to see a different form of biometrics. It's coming in the form of behavioural signatures. So, for example, if I force you to move a mouse on the screen, you will always move the mouse top left to bottom right, for example. But I won't. I'll go in the reverse. So, if I make you press the ST and then the T key on the keyboard, I will record, in exact amount of time, how many nanoseconds it took you to actually do that. You and I will be very different.
Tim: Right.

Dave: So, the way that you operate and the way that you interact with the technology is starting to be monitored to prove it's really you.

Tim: That's really interesting.

Mark: Even down to how you're holding your phone and how you're pressing the thumbprint on your phone as well, right?

Tim: Because they now have pressure-sensing ability.

Mark: Correct.

Tim: That's really interesting. Look, we are going to have to wrap up pretty soon. But before we do, I just wanted to get a bit of an idea on the SOC (Security Operations Centre) that is being built by Accenture here in Australia. What is it?

Dave: Well, basically what we've talked about today, everyone is focused on prevention. And prevention is something that is getting harder and harder to do, and easier and easier for criminals to get into your organisation. So, for those that understand, with things like Zero Day, I didn't get to talk about that, but Zero Day malware, things like fileless malware, they can bypass traditional security controls quite easily and effectively, right? So, in most organisations, you can at some stage breach the perimeter and gain access inside.

So, the idea of prevention, yes, you do it. And you still do it to the best of your ability. But there is a much more of a reliance now on detection and response. So, if someone's in your organisation, you need to detect them quite quickly, and you need to then be able to shut them down, understand what they did, and clean up the mess as fast as you can to recover

Tim: Okay.

Dave: Right? So, what Accenture is doing now is focusing on the detection and response component because it's a very difficult capability to build yourself. It's very specialised, it's very industry leading. You have to keep up with the criminal actors to understand how they break in, what they do when they get in, what sort of techniques do they use?

Dave: So, what sort of - what we call canaries, which is the canaries in the mine - so what sort of canaries would we put in the environment to detect if someone actually had broken in? And then what would we do about it to quickly detect it and shut it down?

Incidentally, sometimes you don't shut it down quickly. Sometimes you want to monitor it for a while just to understand what they're after, how they're going about it, and gain intelligence from it, so that really helps you understand who the actor might be and what they might be after.

Tim: Wow, that's really, really interesting stuff. Look, I think we are going to have to wrap up now. So, Mark, Dave, really appreciate your time. And if anybody who's listening to this wants to dive into any of the areas we've spoken about in more detail, either let us know because I would love to do another recording where we dive into some of these areas because I think we've scratched the surface largely, or just get in touch with us, Mark Leadbetter, Dave Powell, you'll find us all on LinkedIn. And myself, Tim Broome. So, both of you, thanks very much, really appreciate your time.

Dave: Thanks very much, Tim.

Mark: Thanks, Tim.

Tim: Thank you.

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

[End of recording.]