FSR GPS Podcast Series
Episode 15 – Cybersecurity and the impact of AI in financial services

Michael Vrisakis	Hi everyone. I'm Michael Vrisakis, a Partner in the Herbert Smith Freehills Financial Services Team. Welcome to our podcast series called the FSR GPS. This series focusses on topical and emerging issues in financial services regulation which we think are the most strategic and important issues for our clients. Feel free to suggest topics you would like us to cover in the future but for now we hope you enjoy today's episode.
David Kim	Welcome to today's episode of the FSR GPS Podcast Series. My name is David Kim and I'm a Senior Associate in the FSR practice at HSF in Sydney. I specialise in life and general insurance, and regulatory matters. Today I'm joined by Christine Wong and Raymond Sun.
Christine Wong	Thanks David, it's great to be here. I'm a Partner in our Disputes group at HSF and my focus is on supporting clients to respond to crises and investigations, and particularly in the last couple of years that has been increasingly in the cyber and data breach space, as well as more broadly white collar crime and whistleblower issues.
Raymond Sun	Hey everyone. I'm a lawyer in the Technology, Media and Telecommunications team at HSF. I specialise in technology, especially emerging technology and AI or artificial intelligence, commercial contracting and privacy law.
David Kim	In today's episode, we will be discussing cybersecurity laws and the impact of AI in the context of FSR. At HSF, we've noticed an increased focus of regulators and courts on ensuring oversight of cyber resilience and cyber awareness by organisations. To kick us off, Christine, could you give us a background on what is cyber resilience and why is this issue so important for organisations in Australia?
Christine Wong	Sure, thanks very much David. Cyber resilience is effectively the ability for organisations to adapt to disruptions caused by cybersecurity incidents whilst still maintaining continuous business operations, and that includes the ability to both detect, manage and recover from incidents as they arise. As

we saw with CrowdStrike, organisations are becoming more and more interconnected through digital services and that means cyberattacks and outages like the one that occurred with CrowdStrike are becoming increasingly sophisticated and frequent and has the potential to cause increasingly widespread disruption and damage, and for that reason cyber resilience is essential to all organisations operating in the digital economy, but particularly to financial services entities that form a really key part of the way that people need to operate day to day and businesses as well.

So a material cyber incident might cause significant harm to consumers. It might destabilise markets and affect trust and confidence in the financial system. Just to bring a stat that brings this to life, the Australian Cyber Security Centre, or ACSC, estimated that cybercrime cost Australia approximately $42 billion in 2021 and that figure is rising year on year. In an updated report, the average cost of cybercrime per report went up 14% in the 2023 financial year.

David Kim

Thanks Christine. That's very helpful context. What's interesting from an insurance perspective is despite the frequency and severity of cybersecurity incidents, cyber risk is significantly underinsured by organisations. Since the cyber insurance market is relatively young, many organisations have not taken out this type of insurance because of its uncertain return on investment. Currently in Australia, only about 20% of SMEs and 35-70% of larger businesses have taken out a standalone cyber insurance policy. It's really not a well known or a well understood insurance product. On top of that, it's quite expensive. Unlike well-established insurance policies, it's quite difficult for insurers and underwriters to price affordable premiums given the everchanging nature of cyber risk.

Christine, is there a regulatory framework for ensuring oversight of cyber resilience by organisations?

Christine Wong

Great question, David. In short, yes, there is a number of regulatory frameworks and intersecting in some ways, regulatory obligations that sit across businesses and the people that run them to properly manage cyber risk. Those obligations are overseen and enforced by various government departments and agencies, including ones that people would be very familiar with such as ASIC, APRA and the ACSC.

Turning to ASIC specifically, particularly given this audience, ASIC has ramped up efforts in the cyber resilience of financial services and markets.

Recently, it expressed concerns about corporate cyber security measures and the protection of consumer data, and ASIC has announced plans to investigate cyber incidents that cause loss of data from a corporate governance perspective, and have signalled active investigations into directors for breaches of directors' duties in this area.

Some other interesting initiatives that ASIC is pursuing include launching a new threat intelligence platform to promote information sharing and real time detection of cyber threats, as well as implementing a supervisory cyber and operational resilience program, covering areas like use of third party providers, which has been a real focus for ASIC in the context of cyber risks and resilience.

ASIC's focus on cyber risk follows APRA's own release of its prudential standard CPS 230 which relates to operational risk management. That prudential standard is designed to create a sense of urgency for APRA-regulated entities to act on emerging operational and cyber risks posed by new technologies and evolving cyber threats, and both ASIC and APRA have included cyber and data resilience as a strategic priority in their current year corporate plans.

The ACSC has also contributed to the conversation. It recently released a paper called "Questions to the board to ask about cybersecurity" which emphasises cybersecurity risk as a key business risk and guides board directors on how they can manage that.

David Kim

Thanks Christine. And the regulators focus is very much consistent with the enforcement action they've pursued before the court relating to cybersecurity and cyber resilience. Christine, would you be able to take us through the key Federal Court decision in *ASIC v RI Advice Group*?

Christine Wong

Absolutely. So this was a case from 2022, and the first one that ASIC had brought against a financial services entity in relation to cyber-related matters. It was brought against a company called RI Advice, and in short, ASIC alleged that RI Advice had failed to have adequate cybersecurity systems in place which led to a significant data breach. This was ultimately resolved by way of admitted facts and admissions and the Federal Court, in determining the relevant sort of orders to make there, held that in effect Australian financial services licensees do have obligations to adequately manage cybersecurity risks as part of their general financial services obligations under the Corporations Act. So that means putting in place and

---

maintaining adequate risk management systems and procedures to ensure that sensitive consumer information is protected, and to minimise consumer harm. And in that case, the sort of experiences that RI Advice had had over time that put them on notice of various issues and in effect the failures to fix problems as they arose was a key issue.

We have also seen APRA pursue other enforcement activity, but in a different way. So as a prudential regulator it has imposed further capital adequacy requirements on particular organisations that have suffered cyberattacks and where there is perceived deficiencies with their security environment. So for example Medibank had a $250 million increase imposed on its capital adequacy requirements.

David Kim

Thanks Christine. Ray, are there any legal requirements that apply to maintain cybersecurity?

Raymond Sun

Yes, so there is one from a privacy perspective. There's the Privacy Act, which is undergoing reform at the moment. Actually, there was a recent tranche of new amendments proposed that was released in September of 2024, but generally the Privacy Act sets out data protection and privacy obligations that bind many organisations across the board, not just financial sector. And organisations must ensure reasonable steps are taken to protect the collection, use, storage and disclosure of personal information. Generally speaking, the more sensitive the personal information that you handle, the stricter the obligations, and the privacy regulator here, which is the Office of the Australian Information Commission, or also known as the OAIC, they have some pretty comprehensive guidelines on the Privacy Act for organisations to follow.

Christine Wong

And related to those comprehensive guidelines, Ray, they have also commenced civil penalty proceedings in respect of two organisations that suffered cyberattacks. So in the Medibank example and also against a company called Australian Clinical Labs, so it is definitely a space where sort of breaches are being enforced against.

Apart from the Privacy Act, there's also other specific obligations that apply to financial services organisations. So for example, there's prudential standards, like CPS 234, which requires entities who are regulated by APRA to ensure that they maintain information security that is appropriate for the

---

size and extent of threats to information assets, and which also includes a range of other reporting obligations.

Even for financial services organisations that aren't APRA-regulated, there are still the general obligations in the Corporations Act. So – such as the ones I mentioned above in the context of the RI Advice case – which require financial services licensee holders to have adequate risk management systems.

And then finally there's obligations under the National Consumer Credit Protection Act, which requires Australian credit licence holders to have adequate risk management systems in place as well.

David Kim

We might turn to AI now. Ray, this is a topic that you are very passionate about. Maybe for the listeners who are not yet deep in this space, could you tell us what actually is AI?

Raymond Sun

Yeah, sure David.

So AI is really a field of science of building machines to perform tasks that normally require human intelligence. So for example, writing, doing maths or driving cars. There's a lot of terminology around AI but the main one you've probably heard of is "machine learning", which is designing machines to ingest lots of data, find patterns in that data and make predictions based on that data. So apps like ChatGPT, the video feed recommendation on YouTube or self-driving vehicles are all examples of machine learning applications.

David Kim

Yes, thanks for explaining machine learning, Ray. That context is important because it highlights the role of data and therefore privacy and data security in the field of AI.

Raymond Sun

Yeah, exactly. Actually, a very common saying is that "data is like the oxygen of AI".

David Kim

Thanks Ray. Obviously, AI is everywhere today, powering so many apps and systems in our society. I'm sure we could go on and on about the

---

	benefits of AI, but what are some of the legal issues and risks, particularly in the context of cybersecurity in the finance sector?
Raymond Sun	Yeah, so the risk of AI really depends on the particular application or use case of AI. In the financial sector, common AI applications include, you know, fraud detection, automating loan decisions, data analytics, credit score assessments and likewise. So here, AI is predominantly used to automate or streamline decision-making processes which, depending on the context, could affect real customers. One challenge here is known as “data in/data out”. This means any bias in a dataset could seep into an AI’s output decision which, if actioned without proper supervision or if not reviewed properly, could lead to unfair or even discriminatory outcomes.
Christine Wong	Big risk, but also opportunity there Ray, and relatedly speaking of the data that’s used in those systems, they often will include sensitive financial data. So there will also be a privacy and cybersecurity angle at play here, although obviously that’s a universal issue across all IT systems that draw in huge volumes of data, and not just AI.
Raymond Sun	Yeah, that’s right Christine. And there are also some other unique risks posed by AI, especially deepfakes.
David Kim	And by “deepfakes” do you mean the fake images or videos of people generated by AI?
Raymond Sun	Yeah, that’s right. Thanks to advancements in generative AI, deepfakes are getting more realistic and harder to detect, even for machines. Deepfakes could also be used by bad actors to create fake ID, which poses challenges for Know Your Customer sort of processes.
Christine Wong	And it’s not just deepfakes that are an issue but in general, generative AI can be used as a tool to write phishing emails or malware as well.
David Kim	This sounds quite harmful. So what are the regulators saying about this?

Raymond Sun

Yeah, so the Australian government has been running ongoing consultations into AI regulation with the most recent development being a proposal by the government to introduce 10 mandatory guardrails around high risk AI systems and also all general purpose AI models. Now, these guardrails build upon Australia's existing AI ethics principles and also reflect many existing responsible AI practices, and generally speaking, they include requirements like setting up an accountability and risk management process, data governance measures, and also being transparent with end users when you're using AI or producing AI-generated content.

Right now, these mandatory guardrails are subject to public consultation, but in the meantime, the government has also released voluntary guardrails which mostly mirror the mandatory ones which any organisation in Australia can implement right now so that they're better prepared when the mandatory requirements do come in.

The government has mostly made moves in regulating use of AI in the public sector. There's not so much happening yet in the FSR sector, but for FSR sector we've got our existing rules and frameworks which we've been, you know, discussing it just then, that already cover some of the ground in AI.

In terms of regulatory attitudes, earlier this year ASIC Chair, Joe Longo, spoke at a symposium on AI regulation where he said, "Existing obligations around good governance and the provision of financial services don't change with new technology." He also said that, "Current regulation around AI may not be sufficient and ASIC will continue to act within its remit to deter bad behaviour."

Now, as well as contributing to the government's development on AI-specific regulation, under its corporate plan for 2024-2025, ASIC will also be prioritising areas like technology risk and AI, and monitoring licensees' use of AI.

Likewise, APRA has advised in their paper addressing boards that industry should continue conducting due diligence and having appropriate monitoring and robust oversight.

And another example is the OAIC, which I mentioned before. They are also turning their attention to the privacy risks of AI in their latest corporate plan for 2024 and 2025.

David Kim	That's fascinating stuff. Look, that's all we have time for today. Thank you for tuning in to another one of our episodes, and a big thank you to Christine and Ray for sharing your insights with us.
Christine Wong	My pleasure David. Thanks for having us on. I'm just going to do a quick plug as well for our 2024 cyber risk survey that we put out, which surveyed senior legal team members across a range of organisations which I think is really useful reading in this space as well.
Raymond Sun	Thanks David. Great chat.

You have been listening to a podcast brought to you by Herbert Smith Freehills. For more episodes please go to our channel on iTunes, Spotify or SoundCloud and visit our web site herbertsmithfreehills.com for more insights relevant to your business.

END OF PODCAST