Submission to ACCC public consultation

on

Consumer Data Right Rules Framework

Executive Summary

This submission focuses exclusively on the conceptualisation of cyber insurance as part of the accreditation requirements for Consumer Data Right (CDR) data recipients. Given the reliance on the use of Open API to facilitate secure and trusted communications between CDR participants, it would be reasonable to expect cyber insurance to be an element of the overall insurance requirements.

Cyber insurance requirements should be dimensioned to offer sufficient protection to the consumers and CDR participants without overburdening the CDR data recipients. A common concern expressed across a number of submissions to the Review into Open Banking in Australia and Consumer Data Right Exposure Draft is the potential cost burden on the data holders and accredited data recipients, as well as the associated cost/benefit justification.

While there has not been explicit decomposition or dimensioning of these cost structures, there is likely to be a material functional and capacity basis to these cost bases. Cyber insurance requirements, on the other hand, are risk based and have no functional or capacity constraints. They are primarily a policy matter on risk management.

This submission advocates the approach to dimensioning and validating cyber insurance requirements based on the legal concept of "Duty of Care". This approach will minimise the risk of overburdening some potential CDR recipients, especially those from non-profit and social services sectors servicing the disadvantaged. Otherwise it might accentuate the digital divide in our society by discouraging access to innovative services underpinned by the CDR regime and vision.

In addition, such requirements should align with the expressions in the draft ISO Standard 27102[1] on "Information Security Management – Guidelines for Cyber Insurance". This ensures the prescribed requirements are properly understood in an international context particularly given the intent of the CDR framework to include accredited overseas data recipients and to facilitate cross boarder data transfer.

We are members of the Australian Cyber Insurance Think Tank, a coalition of likeminded professionals from across the insurance, cyber risk management and legal services field with 36 current members. The think tank has no commercial or political affiliations and receives no funding. It is not a registered organisation and has no physical presence beyond our LinkedIn group (https://www.linkedin.com/groups/10392474/). The opinions expressed in this submission are of the undersigned and do not represent our employer organisations or related entities. We welcome the opportunities to elaborate on further details in our submission.

[1] https://www.iso.org/standard/72436.html

Nature of Cyber Insurance

Section 6.2.1 in the CDR Rules Framework focuses on accreditation requirements. Page 26 noted that the ACCC welcomes views about the appropriate types of insurance cover such as cyber-attack. Page 26 also cited reference to the European Banking Authority (EBA) guidelines on Professional Liability Insurance requirements. But the EBA guidelines does not cover consideration for cyber insurance requirements. This section explores some of the key challenges in conceptualising these requirements.

According to a recent report[2] from the Geneva Association (GA), cyber insurance is the fastest growing line of business in the insurance industry with estimated global premiums of USD 3 billion. The Geneva Association is the leading international insurance think tank for strategically important insurance and risk management issues. Its membership comprises a statutory maximum of 90 chief executive officers (CEOs) from the world's top insurance and reinsurance companies. The report tabled five challenges: (1) the unique man-made and catastrophic nature of cyber risks; (2) difficulty in measuring and understanding accumulation risk; (3) limited availability and sharing of cyber incidents and claim data; (4) the impact of regulation; and (5) the effect of new technologies on cyber security.

A follow up report[3] focused specifically on the accumulation risk exposure of the industry threatening its viability and sustainability. The primary concern is that a single large event or a series of consecutive events may make affirmative cyber insurance unprofitable. In addition, insurers and reinsurers might have underestimated their non-affirmative cyber exposure leading to an unplanned shock from a major event. And governments might fail to provide a commensurate framework for the sharing of large-scale terrorism-induced losses.

The report noted that "... ***The history of cyber risk is short, and the market has yet to experience a major adverse event. It is vulnerable to risks, and without due attention there is a potential of slipping into undisciplined underwriting*** ...". Given the above analysis from GA, we recommend that the determination of cyber insurance requirements not rely solely on current cyber insurance commercial practices which might be immature and instead focus on market efficiency and competition. It is recommended to also include tests based on the legal concept of "Duty of Care" to consider the effect of these rules on consumer access and minimising digital divide.

Draft ISO Standard 27102

The GA whitepapers cited the challenges of sharing cyber incidents and claims data. A number of barriers were noted, including privacy concerns and maintaining competitive advantage between insurers. The lack of standardisation and understanding of cyber insurance policies both globally and within specific geographic markets is a direct consequence of this situation. This represents a material challenge to ACCC in drafting cyber insurance requirements based on practices and offering from the local cyber insurance industry. It could result in inconsistent application of these requirement rules and mis-leading and deceptive conducts by some rogue operators.

[2] https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/cyber_insurance_as_a_risk_mitigation_strategy.pdf
[3] https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/report_advancing_accumulation_risk_management_in_cyber_insurance.pdf

The draft ISO Standard 27102 [4]attempts to address this knowledge gap. The stated goals are:

> ***(a) assisting information security professionals use cyber insurance as an option for risk treatment;***
>
> ***(b) sharing of data and information between an insured and insurer to support underwriting, monitoring and claims activities associated with a cyber insurance policy;***
>
> ***(c) leveraging cyber insurance to help manage the impact of a cyber incident;***
>
> ***(d) leveraging an ISMS to share relevant data and information with insurers.***

This draft standard is expected to be published at end of 2019. Given the expression in the latest draft (published in June 2018), it is unlikely that the final published standard will contain any specific reference to the concept of consumer data right or open banking as a use case. However the ACCC can consider taking advantage of the expression in the draft standard when formulating its cyber insurance requirement rules. Such alignment will minimise confusion from differing interpretations of specific terms and concepts in the consumer market place when the standard has been released.

The Australian Cyber Insurance Think Tank

We are members of the Australian Cyber Insurance Think Tank. It is a coalition of likeminded professionals from across the insurance, cyber risk management and legal services field with 36 members currently. It has no commercial or political affiliation and receive no funding. It is not a registered organisation and has no physical presence beyond our LinkedIn group (https://www.linkedin.com/groups/10392474/). The immediate focus of the group is to conceptualise the local adoption of the draft standard in Australia when it is expected to be released at end of 2019. Members of the Think Tank have made submission to the draft standard.

The professional composition and independent nature of the Think Tank makes it well suited to offer advice to the ACCC in the drafting of cyber insurance requirements in the context of ISO Standard 27102.

Duty of Care requirements

Given the industry challenges discussed in previous sections in conceptualising cyber insurance, we advocate to include some tests based on the legal concept of "Duty of Care[5]". In general, insurers have no duty of care to policyholders unless they provide advice to them or unless the contract itself breaches the law. Insurance brokers can have some duties for example to advise appropriately, but Insurance itself has certain protections provided by the Insurance Contracts Act and other legislation. In particular it is exempted from the Australian Consumer Law.

[4] https://www.iso.org/standard/72436.html
[5] https://en.wikipedia.org/wiki/Duty_of_care

The Duty of Care Standard (DoCRA[6]) offers a structured approach to apply the duty of care concept for assessing cyber security risks. It is based on three core principles:

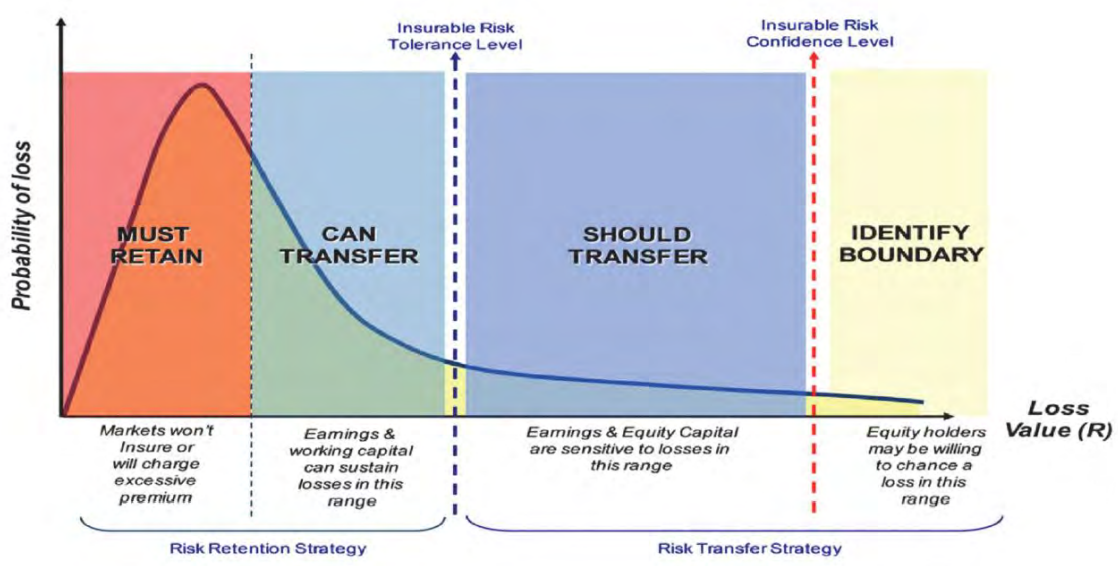
1. Risk analysis must consider the interests of all parties that may be harmed by the risk.
2. Risks must be reduced to a level that authorities and potentially affected parties would find appropriate.
3. Safeguards must not be more burdensome than the risks they protect against.

This approach has been successfully applied to a global cyber security standard CIS RAM[7] published by the Center for Internet Security (CIS). Such an approach might also form a useful framework to conceptualise cyber insurance requirements reflective of the cyber risks to be covered.

Cyber Insurance as a Risk Language

The CDR rules framework stated that it does not outline the proposed drafting for particular rules. Rather, it outlines the substantive and/or 'in principle' position the ACCC proposes to take when making rules. To this end, we advocate the concept of "Cyber Insurance as a Risk Language".

Insurance is a risk transfer mechanism. As discussed in the GA whitepapers, a major challenge to cyber insurance in measuring and understanding accumulation risk. The following diagram extracted from the whitepaper "An Efficient Tool for Catastrophic Losses"[8] illustrates the impact on insurability from defining the "Insurable Risk Tolerance Level" or "risk boundary":

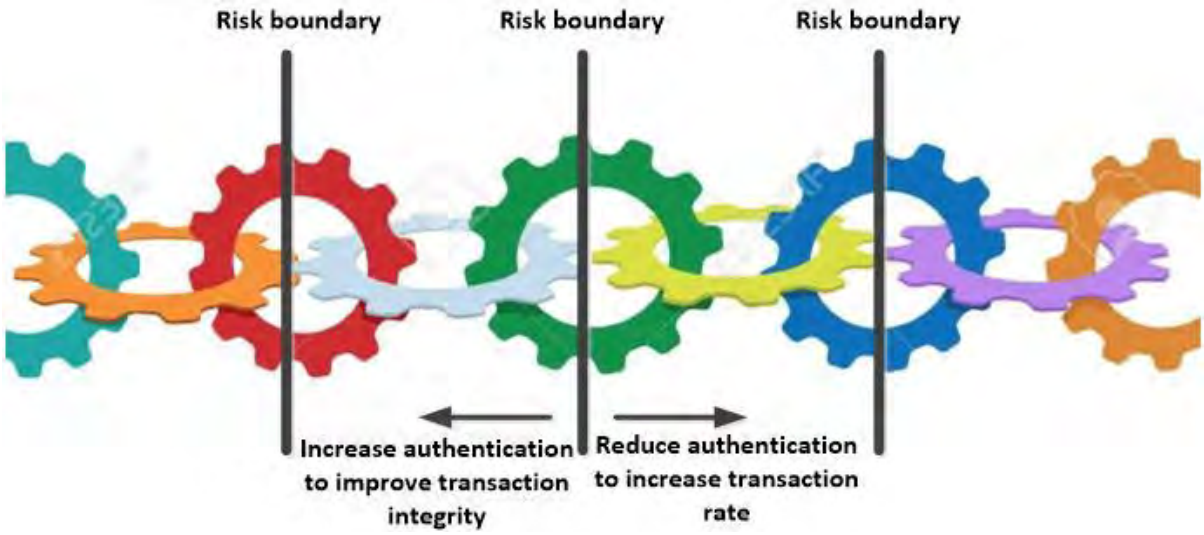


Insurance policy, by itself, does not alter the nature of risk nor reduce its impact. The insurers and insureds negotiate these "risk boundaries" according to their own risk appetites and risk mitigation capacities. A common example of such negotiation comes in the form of policy excess and inclusions/exclusions. As discussed in the GA whitepapers, insurers are increasingly offering cyber risk

[6] https://docra.org/
[7] https://learn.cisecurity.org/cis-ram
[8] https://www.im.jlt.com/-/media/files/sites/im/anne-marie-towle--captives--an-efficient-tool-for-catastrophic-losses-january-2018.ashx

services citing the following benefits: (1) increasing attractiveness of cyber insurance for customers; (2) improving profitability through loss reduction/prevention and customer retention; and (3) gaining cyber risk knowledge. In other words, the insurers are working collaboratively with the insured to shift the "risk boundaries" to reduce the potential cost of the risk exposure.

A specific characteristic of information dense supply chains such as those targeted by CDR is the presence of commodity information elements which can be transferred readily along the supply chain as depicted below:



Digital identity management is a common information commodity which can be traded along a supply chain. The key concepts of consent, authentication and authorisation in the CDR framework apply to digital identity management. Delegating these processes to information aggregators and brokers is common practice in the industry today which creates challenges in managing liability and can have material implications on cyber insurance coverage. Cyber Insurance can be conceptualised as a Risk Language to describe risk boundaries to support the negotiation of the policy coverage. Our submission advocates that "Duty of Care" considerations should be balanced alongside commercial objectives. We welcome the opportunity to deliberate further.

Conclusion

Cyber insurance is an important element in the insurance requirements in the accreditation rules for CDR data recipients given the dependence on the use of Open API to facilitate secure and trusted data transfers. Recent research from the Geneva Association tabled the many challenges faced by the cyber insurance industry to ensure profitability and sustainability. This submission advocates the need to balance commercial objectives against social obligations in ensuring discharge of "Duty of Care" to the consumers. The Duty of Care Standard (DoCRA) might be a practical framework for developing suitable tests to assess the sufficiency of the accreditation rules. Cyber Insurance can be conceptualised as a Risk Language to describe such risk boundaries to support negotiation of the policy coverage.

This submission is submitted by members of the Australian Cyber Insurance Think Tank which is a coalition of likeminded professional in the insurance, cyber risk management and legal services fields. It has no commercial nor political affliction. The opinion expressed in this submission are of the undersigned and do not represent our employer organisations or related entities.

Co-authors of this submission (in alphabetical order)

Ahmed Khanji[9] - Chief Executive Officer, Gridware Cyber Security

Andrew Wan[10] – Chief Information Security Officer | Head of Security

Branko Ninkovic[11] - Cyber Security - Founder Dragonfly & VAXXIN8, Speaker and Mentor

Chris Cronin[12] - Author of the DoCRA standard. Information Security Consultant / Risk Management Leader

Christophe Doche[13] - Executive Director of The Optus Macquarie University Cyber Security Hub

Christopher Lynam[14] - Insurtech | Cyber | Director & Co-Founder Edmund Insurance

Dennis Rodrigues[15] - Cloud | Security | Devops

Denny Wan[16] - Cyber security risk expert and postgraduate researcher into cyber insurance pricing strategies

Gary Bone[17] - CISSP and Security Consultant at TERCIO

George Newhouse[18] - Adjunct Professor at Macquarie University & Director at The National Justice Project

James Crowther[19] - Agile Underwriting General Manager - Cyber. Founder, Director at DARC

John O'Brien[20] - Insurance Placement Broker specialising in emerging technologies

Petra Wildemann[21]– Actuary, cyber risk expert and into digitalisation transformation topics

Richard Smith[22] - Co-Founder, Edmund, Radically fast cyber insurance

Rowena Cheung[23] - Consulting | Project Management | Business Analysis | Payments

Shelvin Narayan[24] - BurMac Cyber Solutions

Tahiry Rabehaja[25] - Postdoctoral Research Fellow in cyber security risk quantification

---

[9] https://www.linkedin.com/in/ahmed-khanji/
[10] https://www.linkedin.com/in/wanand/
[11] https://www.linkedin.com/in/branko-ninkovic-4527891/
[12] https://www.linkedin.com/in/chris-cronin-351416/
[13] https://www.linkedin.com/in/christophe-doche-b49408120/
[14] https://www.linkedin.com/in/christopher-lynam-b2178084/
[15] https://www.linkedin.com/in/dennis-rodrigues-bb3364a/
[16] https://www.linkedin.com/in/wandenny/
[17] https://www.linkedin.com/in/garybone/
[18] https://www.linkedin.com/in/georgebnewhouse/
[19] https://www.linkedin.com/in/james-crowther-62238618/
[20] https://www.linkedin.com/in/john-o-brien-41445043/
[21] https://www.linkedin.com/in/petra-wildemann-1b6798/
[22] https://www.linkedin.com/in/richard-smith-203147145/
[23] https://www.linkedin.com/in/rowena-cheung/
[24] https://www.linkedin.com/in/shelvin-narayan-4a4b5433/
[25] https://www.linkedin.com/in/tahiry-rabehaja/

Tawanda Mangere[26] - Risk Management Leader / Fintech- Payments Industry Specialist

[26] https://www.linkedin.com/in/tawanda-great-mangere-38b64512a/