Cisco Systems Australia Ltd.

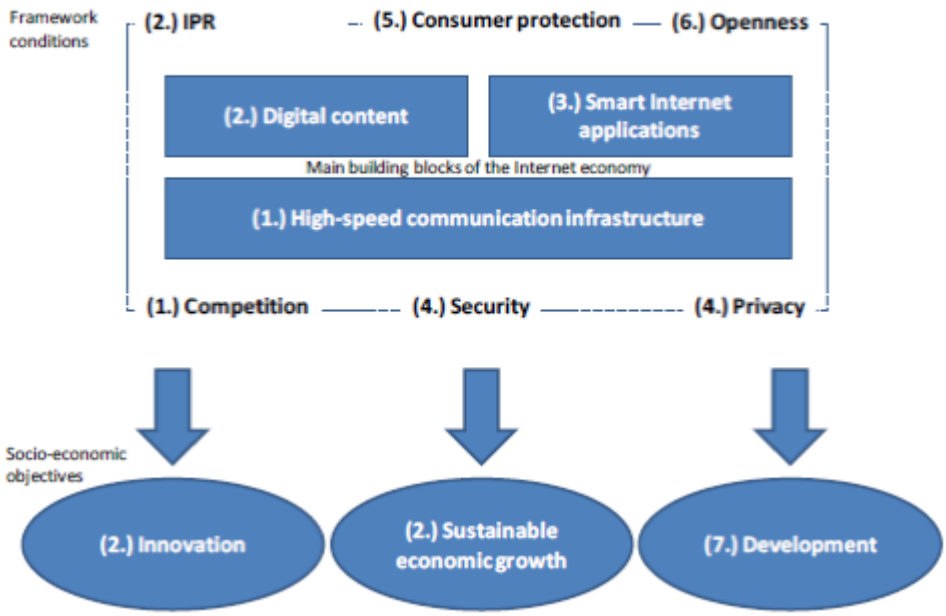
Interim Submission to the Financial Systems Inquiry

Appendix

1. Trust and confidence in the digital future of banking

Banking and financial services are built on Trust and Security. The future of the industry will depend implicitly on initiatives to retain and enhance the trust and confidence of all stakeholders. This dependence will evolve and become more nuanced with the increasingly rapid and pervasive adoption of digital technology across the sector. In this context, Cisco would like to draw the Inquiry's attention to the OECD's Internet Economy Model (refer Review of the Seoul Declaration for the Future of the Internet Economy)[1].

Figure 1. Analytical framework for reviewing the seven themes of the Seoul Declaration



Whilst all aspects of the model are in fact relevant to the Inquiry's terms of reference we wish to highlight the following:

- Cyber security;
- Privacy;
- Consumer protection and empowerment; and
- Openness.

Boston Consulting Group[2] has attempted to model the economic value of trust, projecting a 'trust dividend' of as much as US$1 trillion within the G20 online retail economies in

[1] http://www.oecd-

[2] http://www.bcgperspectives.com/content/articles/financial_institutions_digital_economy_trust_dividend/?chapter=2

2016 with eroded trust delivering a total of US$1.5 trillion in sales whereas enhanced trust could deliver as much as US$2.5 trillion in sales.

Similarly, Melissa Hathaway's research[3] with the Belfer Center for Science and International Affairs, at Harvard's John F Kennedy School of Government, has revealed that hostile cyber activities have significant potential to erode GDP growth. For example, the Netherlands has reported that cybercrime costs Dutch society at least €10 billion per annum, or nearly two percent of national GDP. Germany and the United Kingdom report similar losses. The United States estimates the annual impact of international IP theft to the American economy at US$300 billion or one percent of its GDP. In terms of Australia's exposure, this study reveals that Australia is one of the five most mature cyber economies (the others are Canada, the Netherlands, the United Kingdom and the United States of America) but that even these five countries are not truly cyber ready when assessed according to the research criteria for cyber readiness.

In Cisco's 2014 Annual Security Report[4], we note that "the exploitation of trust is a common mode of operation for online attackers and other malicious actors. They take advantage of users' trust in systems, applications, and the people and business they interact with on a regular basis." The evidence suggests that these types of attacks are constantly evolving with new, ever more sophisticated attack methods. Of course, the financial service sector and its customers are a prime target for any attacks motivated by financial gain.

When looking to the future, various commentators point to the anticipated exponential growth in Internet-connected devices and the advent of the so-called 'Internet of Things' (IoT) or the 'Internet of Everything' (IoE). Like every advance in Internet technology, the IoT or IoE has the potential to be used for good or evil. Simply put, innovations in this area have the potential to enrich humankind but can also be used to disrupt the Internet which has become an essential element of the social and economic fabric of the modern world - no more so than in the context of the banking and finance sector's reliance on the Internet and associated mobile platforms for the delivery of products and services, real-time trading platforms, and domestic and international funds transfer.

2. Australian banking technology – a current assessment

Australians benefit from one of the most stable and highly/advanced secure banking and finance systems in the world, underpinned by well-managed and in the main, robust (although ageing - refer Section 3.1 below) technology platforms. Availability of services is high and e-fraud and identity theft rates are low by world standards. The level of cooperation among competing financial institutions is mature and effective and boards generally recognise the need for broader sectoral cyber resilience to complement their own organisations investments in cyber capabilities.

Much of the core banking technology still in operation today was introduced up to 40 years ago, although some banks have addressed or are addressing this problem. However, others have yet to do so and the sector's continued reliance on ageing technology platforms presents a current and significant emerging risk to the resilience and stability of

---

3 http://belfercenter.ksg.harvard.edu/publication/23607/cyber_readiness_index_10.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%253A+belfer%252Fscience_technology_and_public_policy+(Belfer+Center+for+Science+and+International+Affairs+-+Science%252C+Technology%252C+and+Public+Policy)

4 https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf

banking services. The same is true of other parts of the financial sector such as wealth management where the problem is exacerbated by long term products (e.g. superannuation and life insurance products) administered through ageing technology platforms[5].

This will present as future risk in two aspects – the first being the increasing incidence of failure of legacy technology, and the second being project delivery risks and the likelihood of unplanned disruptions to services as banks undertake the huge modernisation programs required to replace legacy technology platforms.

However, notwithstanding the legacy technology risk which it bears, the Australian banking and finance sector has proven its innovative credentials and capabilities - it has an enviable track record. The delivery of Internet and mobile banking services by Australian banks is world-leading in terms of both innovation of the service and focus on the underlying security paradigm. Similarly, EMV adoption is now almost complete (with the August 2014 move to mandatory chip and PIN) and contrasts significantly with the recognised international laggards in EMV adoption such as the USA which is only now moving to chip and signature.

Adoption of digital channels has seen traditional channels and payment instruments decline in usage in Australia to the point where some can, and should be retired (e.g. cheques) within the next decade and others like ATMs have already passed their peak in terms of both the number of ATMs and their utilisation. The retirement of these traditional methods needs careful planning to balance the cost savings to the industry with the potential unintended impacts on certain customer groups, some of which may require industry-sponsored assistance to migrate to contemporary banking methods. The cost of this industry assistance should therefore be factored into any business cases relating to broad industry plans to retire legacy banking services.

3. Current and emerging risks

3.1. Legacy technology risks and transformation risks

As noted above, participants within the Australian banking sector are at varying stages in terms of their initiatives to retire and replace legacy systems that have been in operation for decades. The same is true for the wealth management industry that protects the retirement wealth of all Australians.

To date, the decision to replace ageing technology or defer such projects has been left to the boards and management teams of the individual financial institutions although APRA has maintained careful interest in the threat profiles of individual institutions. Going forward, this growing threat to system stability may need to be reassessed, especially in the context of any banks that are deemed systemically significant in an Australian context.

3.2. Australian banking sector – an essential part of Australia's Critical Infrastructure

In the intervening years between the Wallis Inquiry and the current Murray Inquiry, the concept of national 'critical infrastructure' has come into being. In Australia as with other advanced nations, the banking sector has been formally included within the country's critical infrastructure portfolio. Accordingly, any proposed changes to the regulatory environment in which the sector operates, needs to take this significant

[5] http://www.apra.gov.au/Insight/Pages/APRA-Insight-Issue-1-2013.aspx

national security context into account. Ideally, this should be one of the key lenses within a formal impact methodology as recommended under Section 4.1 of this Appendix.

3.3. Threats to the banking sector arising from challenges to the multi-stakeholder model of Internet governance

The banking and finance sector is a key stakeholder, both in an Australian context and globally, in relation to the proper governance of the Internet. Although this may appear self-evident, the importance of this relationship between Internet governance and the resilience and reliability of the banking system is not evidenced in terms of the sector's engagement in the Internet governance debate to date. Quite simply, with very few exceptions, financial institutions have considered Internet governance advocacy to be the responsibility of governments, Internet registrars, telcos and civil society organisations (such as the Internet Society).

However, failures in Internet governance have the potential to undermine the digital economy of which banks are key participants and as such, the banking sector should recognise its role in influencing the considered evolution of the multi-stakeholder model of Internet governance. This critical link between the prospective health of the banking and finance sector and the forces that govern the Internet should be recognised and addressed.

3.4. Contagion and systemic risk scenarios

The makeup of the Australian banking sector bears a similarity to the Canadian banking sector. In both markets, four banks are systemically significant due to their collective market share.

In recent years, we have witnessed sustained periods of systems outages suffered by one or other of the major banks such that they have been unable to effectively participate in exchange and settlements across the various payments systems. The most notable (and damaging) incident involved an extended outage suffered by one of the Australian majors affecting payments for over a week with a consequent impact on customers of not only the bank in question but also on customers of all other banks.

Extrapolating from these events, it can readily be appreciated that the impact on the Australian economy could be devastating if two (or more) of the majors were to simultaneously sustain prolonged systems outages. Such a scenario could be instigated by a range of intentional (i.e. malicious) and unintentional events.

In terms of intentional acts, these could be instigated by either state or non-state actors with an intent to damage Australia's economy through attacks on the nation's critical infrastructure. Hostile actors could seek to achieve their objectives through direct physical attack on critical infrastructure or through network based attacks, for example directed at SCADA supervisory systems that manage major technology installations and the supporting infrastructure or alternatively via sustained denial of service attacks such as those to which the USA banking sector has been subjected over the past two years.

In terms of unintentional events, these could arise through the banking sector's reliance on common providers (e.g. telcos, technology providers or energy providers). Of course there is always the less likely but still plausible scenario in which two or more institutions are simultaneously impacted by events with entirely unique root causes. In the World Economic Forum's ninth Global Risks Report (2014 edition) environmental triggers are also recognised - such as earthquakes, solar super-storms as well as the increasing threat posed by space junk to working satellite systems.

This extreme scenario could have implications for the 'Four Pillars' policy in that relaxation of the policy would need to take into account the potential to exacerbate this risk.

When assessing the broader context of this extreme scenario, it is important to recognise that the RBA's own role in the payments systems is such that the scenario is likely to hold true in the event that it was one of the two (or more) financial institutions that was to be simultaneously impacted. In fact the inclusion of the RBA should be considered a special case given its particular role as noted in Section 3.5 below.

3.5. Specific risk scenarios

The Australian banking and finance sector contains some unavoidable single points of failure such as those systems operated by key industry participants (e.g. the RBA (RITS and prospectively, the NPP hub), Austraclear and the Australian Securities Exchange.

These are specific risks inherent in the structure of the Australian financial market but are nonetheless significant as a prolonged operational failure by any one of these participants could have a severe impact on the whole financial sector and the broader Australian economy. Such failures would constitute true 'black swan' events for which the financial services industry needs to prepare for. Having a playbook that details a response on how to defend, protect and restore identified roles/responsibilities for recovery/alert is an imperative.

3.6 Hyper-connectedness and cyber resilience

Cyber mature enterprises must recognise that their own cyber resiliency as well as that of the customers and communities they serve depends implicitly not only on their own internal cyber capacity but also on how they actively engage with others in their industry together with their customers, providers and government to promote cyber resilience and to collaborate in planning, preparation and response to cyber events beyond the ability of individual enterprises to contain or resolve.

This aspect of resilience is at least as important as the technical security capacity in which financial institutions may already invest and requires recognition of the need at the board level.

The World Economic Forum has proposed a partnership for cyber resilience model that whilst essentially voluntary, should be both adopted by financial institutions and actively promoted by them to their stakeholders such as their customers and their service providers.

The financial services sector also needs to recognise the ongoing need for active public-private sector collaboration to achieve both sectoral cyber resilience as well as broader national cyber resilience. In the past, some financial institutions contributed personnel to resource the Australian High Tech Crime Centre within the Australian Federal Police and whereas this no longer occurs, there is currently a dialog emerging with the Attorney General's Department and the newly formed Australian Cyber Security Centre to determine the feasibility of establishing a banking sector function within the ACSC, funded by the banking sector. Cisco believes this to be a logical model and one that will underpin the essential public-private sector partnership between the government agencies and the financial sector stakeholders that have an interest in containing and responding to cybercrime.

Cisco recommends that the Inquiry review the FS-ISAC which was established by the US financial services sector in response to 1998's Presidential Directive 63. That directive -

later updated by 2003's Homeland Security Presidential Directive 7 - mandated that the public and private sectors share information about physical and cyber security threats and vulnerabilities to help protect the U.S. critical infrastructure.

Constantly gathering reliable and timely information from financial services providers, commercial security firms, federal/national, state and local government agencies, law enforcement and other trusted resources, the FS-ISAC is now uniquely positioned to quickly disseminate physical and cyber threat alerts and other critical information to member organisations. In recent times, Australian banks have been discussing the merits of forming a local chapter of FS-ISAC.

3.7. International standards – adequate or not?

Over the years, APCA has demonstrated a capacity to balance the need to establish rigorous technology standards which reflect world's best practice with the need to do so in a transparent framework that promotes both confidence and competition. As a consequence, Australian banking customers benefit from highly interoperable payments systems that are safe and highly secure. New market entrants and technology partners have similarly benefited from the transparency and objectivity with which APCA discharges its obligations to the industry.

The role of APCA in the efficient and effective functioning of a vibrant and competitive financial services industry should not be taken for granted. To do so would be to expose Australian banking and financial services customers to uncertain quality and potentially higher costs arising from closed and potentially flawed technology deployments by both established financial institutions and new market entrants.

3.8. Cyber capacity building - a crisis in the making

Increasingly, even the best funded and resourced financial sector cyber teams are experiencing difficulties in recruiting qualified and competent security professionals. Anecdotally, some roles have remained vacant for 12 months or more while management teams actively attempt to find the right staff. This is a common refrain and one which has been recognised by the UN's Governmental Group of Experts in their most recent report on cyber[6].

It has also been recognised in Cisco's 2014 Annual Security Report[7]: "The security talent shortage makes this problem worse: even when budgets are generous, CISOs struggle to hire people with up-to-date security skills. It's estimated that by 2014, the industry will still be short more than a million security professionals across the globe."

This problem is well recognised within the Australian academic sector. Declining student enrolments and a lack of both public and private sector funding for Australian cyber research are now reaching critical levels. Given that the financial services sector is the largest employer of this scarce talent pool, this is an issue that the Inquiry needs to recognise as a problem requiring a considered response.

4. Current and future innovation

4.1 Innovation through relaxing the barriers to entry

Previous initiatives to increase competition have not necessarily achieved their objectives and have in some instances delivered unintended consequences such as potentially

[6] http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98
[7] https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf

increasing risks to stability, adversely impacting customers and entrenching reliance on cash (e.g. ATM ownership and interchange fees, credit card surcharge regime).

Accordingly, Cisco recommends that any consideration to modify the regulatory regime should be accompanied by a full impact assessment that recognises the both the intended and unintended consequences of regulatory change. Ideally, the Inquiry should consider the establishment of a formal impact methodology to ensure that the process of impact assessment is transparent and informed.

4.2 Digital identity

Online and mobile banking services rely on a high trust relationship between financial institutions and their customers. Trusted identities are essential for non-repudiation and to date these are established on a unique basis (i.e. unique between a particular financial institution and a particular customer of that institution). This places a burden on customers with relationships with multiple financial institutions in that they are required to enrol and maintain a set of unique identity profiles.

This is a problem that has been universally recognised and through public and private sector partnerships, other countries are developing robust federated identity frameworks that enable their citizens to use a common identity profile(unique to each individual) to transact with government agencies, banks and other relying enterprises. The USA, UK and Canada are perhaps most advanced in the development and deployment of such federated identity frameworks and whereas the Australian Commonwealth Government has established the Reliance Framework, it is only in its early stages of roll out and adoption by government agencies and has had only limited input from other potential relying parties such as banks.

In the absence of such a framework, other non-financial sector enterprises, notably social media organisations are establishing identity services none of which are likely to be able to offer the identity assurance required by governments or the banking and finance sector. Essentially, federated identity frameworks require the consideration of a hierarchy of trust whereby the identity asserting party should be able to provide assurance as to the veracity of an individual's identity to a level that meets or exceeds the needs of the identity relying party (including identity attribute assertion which preserves the privacy of the owner of the identity profile by revealing only those attributes on which the relying party wishes to place reliance).

As can be seen from the above commentary, identity frameworks are complex and none more so than federated identity frameworks. They are also expensive which is why the international initiatives that have had the most traction to date are those in which the national government has established a framework and then contracted with the private sector (generally banks and technology providers) to deliver the technology and systems to instantiate the federated identity services.

The Inquiry should recognise the growing importance of federated identity to the delivery of digital services and advocate for the extension of the Reliance Framework to achieve both the needs of government and other asserting and relying parties such as banks and other providers of financial services.

In this context, we also note the importance of the Commonwealth Government's Digital Verification Service (DVS) which seeks to provide an online source of trusted identity material derived from both Commonwealth and state government identity asset databases (e.g. births deaths and marriages, drivers' licenses etc.). The Auditor-General has noted

that the DVS has been challenged by data quality issues in the contributing state government databases and this situation is likely to prevail with a consequent diminution in the value and integrity of the DVS service and as such, is a critical prerequisite that ought to underpin a government-sponsored and private sector run, federated identity framework.

There is also a specific practice about which the Inquiry should be aware relating to the way in which so-called account aggregators encourage bank customers to contravene the terms and conditions of their online banking relationships with their banks. In general, account aggregators use a practice known as screen scrapping to intermediate logons to customers' bank accounts via their (i.e. the aggregators') portals. Identity protocols exist (and could be implemented via a government-supported federated framework) to obviate the practice of screen scrapping and this is key concept of which the Inquiry should be aware.

4.3 Consumer attitudes to privacy and personal data in the era of big data

The Office of the Australian Information Commissioner's 2013 report on Consumer Attitudes to Privacy ranks banks as second only to the health sector in terms of consumers' trust and confidence regarding privacy. Notably, the sector improved in ranking from third (behind health and government) in the prior (2007) survey.

This is an extremely positive outcome - one which the banking sector needs to recognise and value. Notably, the social media sector ranked lowest in the latest survey and this is significant in that social media enterprises are most evident in their initiatives to monetise their vast user bases through entry to the financial sector. To the extent that this is permitted by regulatory change, there is a very real risk that the community's trust and confidence in the sector could be diminished. Essentially, all new market entrants should be required to adhere to the principles and standards that have enabled the banking sector to achieve its enviable ranking in the current OAIC survey - rather than allowing a 'race to the bottom'.

The value and control of personal information is also undergoing significant revaluation - nowhere more so than in the UK where the government's 'midata' initiative has been established to provide consumers with access to their personal data held by financial institutions (among other enterprises that hold similarly large amounts of personal information) in a format that will enable them to make better-informed financial decisions. Cisco believes that Australian consumers could benefit from a similar initiative to which we would encourage the Inquiry to give special consideration.

4.4 Financial Services adoption of cloud

As noted in 'Advancing Australia as a Digital Economy' issued by the Commonwealth Government in June 2013, the National Cloud Computing Strategy was established to address barriers to adoption while maximising the benefits of cloud computing in Australia. The strategy includes a series of actions which among others include the following that are particularly relevant to the banking and finance sector:

- support a vibrant cloud sector—this will include ongoing collaboration between the Government and industry;
- promote Australia as a trusted hub for data storage and processing, while encouraging foreign investment and participation.

Due to their substantial compute needs, banking sector participants are ideally placed to be anchor tenants of a domestic cloud industry with export potential and which could

underwrite Australia's digital future. Similar initiatives are being discussed in the UK where the Royal Bank of Scotland has proposed the concept of a financial services cloud[8] and has cited the adoption of cloud technologies by the US healthcare industry with similarly sensitive information.

Cisco has announced a $1 billion investment in a global Intercloud to cost-effectively and quickly deliver business applications and services. This will include Australian-based infrastructure and services to be delivered in conjunction with local partners such as Telstra.

4.5. Payments system reform

The New Payments Platform (NPP) is an important Australian financial services industry response to the RBA's Strategic Review of Innovation in Payments Systems which was completed in 2012. Cisco endorses the rationale that underpins the strategic review which is that market forces are normally sufficient to promote innovation except in those circumstances which are system-wide or cooperative in nature across multiple stakeholders and which based on past experience (e.g. Mambo) have proved to be difficult to achieve. By setting out the clear context for the strategic review in these terms, the RBA has demonstrated its in-principle confidence in market forces in all other circumstances.

4.6. Mobile wallets and payments intermediaries

Australian financial institutions are among the world leaders in safe and highly secure adoption of mobile technologies to deliver a diverse range of products and services to all customer segments. A number of major banks now report that over 60% of online transactions are conducted by customers using mobile devices.

Some institutions are now working on the development of mobile wallets with advanced security the expectation that within the planning horizon of this Inquiry, these solutions could substantially though probably not completely, replace the need for physical cash and coins. As with the current generation of mobile financial platforms, Australia is very likely to lead in the adoption of digital wallets and as consequence there may be relatively few opportunities to learn about the broader economic, fiscal and social impacts from similar initiatives in other countries.

Accordingly, the Inquiry might consider the need to model the impacts of a broad based adoption of digital wallet platforms. Additionally, interoperability as well as safety and enterprise grade security of these platforms will be essential if the replacement of a universal payment instrument such as physical cash and coins is to be feasible. As such, this may be an area in which the Inquiry might consider the need for industry standards and this would most likely fall into the remit of APCA. Cisco strongly encourages the Inquiry to espouse the support of standards to encourage adoption, innovation and greater economic impact.

Obviously the adoption of an interoperable digital wallet will require consideration of the opportunities and challenges posed by digital identity (ref Section 4.2) and virtual currencies (ref Section 4.7).

---

[8] http://www.techradar.com/au/news/internet/cloud-services/rbs-floats-idea-of-uk-financial-services-cloud--1234469

4.7. Virtual (crypto) currencies

Cisco recommends that the Inquiry recognise that virtual (or crypto) currencies are relevant to its terms of reference. At this stage, all virtual currencies present as speculative commodities rather than true currencies but this could change - especially if one or other virtual currency was to be regulated.

In recent times, even without regulatory oversight by any financial regulator, and notwithstanding the recent Mt Gox receivership, virtual currencies have found their way into everyday commercial transactions around the world. There are businesses that accept virtual currencies from their customers and pay their employees in the same way. Conceptually at least, virtual currencies are technically sound (depending on the integrity of the underlying algorithm) and the concept has been made more legitimate by virtue of the quantitative easing to which governments have resorted to increase money supply in traditional currencies - especially post GFC.

However, it's not just retailers that are beginning to bring legitimacy to virtual currencies. A leading USA bank, JP Morgan Chase is proposing a new crypto-currency payment system that would compete with debit and credit cards as the predominant way of making online transactions. To achieve this objective, JP Morgan Chase has filed a USA patent application for a computerised payment system that approximates a virtual currency.

Virtual currencies will no doubt increase in relevance over the next decade as the concept of digital wallets achieves mainstream acceptance, and as the role of physical notes and coins diminishes in day-to-day commerce. The promise of reducing fraud and the associated cost that is borne out by consumer fees is one benefit that may surface. An additional attraction from a government 'tax take' perspective is that properly regulated, a virtual currency could ensure greater GST and income tax compliance and enhanced monitoring of transactions by Austrac.

5. The legal framework and role of law enforcement

Australia's legal framework should play a role in deterrence through presenting Australia as a tough place for cybercriminals to do business and there are series of initiatives that have either been completed or are in train that will contribute to that objective. However, as outlined below there are some issues that should cause the banking and finance sector some concern in regard to Australia's ability to report, prosecute and convict the perpetrators of cybercrime.

The Commonwealth Government ratified the Council of Europe's Cybercrime Convention on 1 March 2013 and published the National Plan to Combat Cybercrime later in 2013. Both of these initiatives are critical in terms of the global and escalating nature of cybercrime.

A point of note however, is that there must be some doubt as to whether the ACORN system (intended to enable victims to report crimes) which is being developed by CrimTrac will achieve the purposes for which it is intended.

Another point of concern relates to the specific cyber capacity building needs relating to achieving suitably cyber-aware judiciary and prosecution teams across all jurisdictions in Australia. Along with the current shortage of recognised cyber expert witnesses, deficiencies in the required cybercrime skills and expertise will potentially make it harder than it ought to be to achieve convictions for cybercrime. Cisco has a long history of investing to address shortages in IT skills via our Networking Academies. Cisco recommends that the Inquiry focus on a similar investment in IT based skills to address these shortages as a priority.

6. Regulation

6.1. Regulation and prudential oversight

The Australian financial sector has performed significantly better than most over the period since the Wallis Inquiry and this must be attributable in no small measure to the regulatory regime that was shaped by that inquiry.

It is hoped that changes in the regulatory oversight of the financial services sector as a result of the current Murray Inquiry will be as insightful and successful in charting a course between principles-based prudential oversight and definitive rules-based regulation and legislation. In this context, we are aware that Cisco's own insights and recommendations need to be critically examined along with other submissions to ensure that collectively, the balance is not unduly weighted one way or the other. We strongly recommend that this lens should be applied to the portfolio of initiatives that will critically inform and influence the regulatory environment over the ensuing years post the current inquiry.

6.2. The role of key regulators with regard to cyber and privacy risks

The financial services industry is subject to regulatory oversight by APRA, ASIC and the OAIC in terms of cyber and privacy protections afforded to customers. Current cyber and privacy regulatory principles, standards and guidance are adequate when coupled with recognised IT industry security standards (e.g. Australian Signals Directorate Top 35, ISO 27000 series, ISO 13569, NIST framework etc).

Considerations should be given to a breach notification regime. Essentially, the banking and finance sector and importantly, customers of all financial institutions would be the net beneficiaries of a breach notification regime because evidence to date suggests that breaches of non-financial systems (social media, retail merchants) contribute to identity theft and takeover activities that can then be used to target the victims' financial holdings.

7. Next Steps

The opportunity for the Inquiry to build upon Australia's current strengths and deepen the economic moat for future generations is tremendous. We are operating at the intersection of a 'perfect storm' made up of people, processes, things and data being connected at an unprecedented rate. Technology is the glue that is binding all of these elements together and enabling new and innovative ways for Financial Services to respond in this digital age.

Our submission has called out the following areas for focus:

1. Internet of Everything and the impact connectivity has on GDP
2. Cyber Security: Threat and Opportunity
3. Cloud Adoption: Australia as a trusted hub for data storage and processing
4. Cyber Skills Shortage: Investment to create required skills
5. Judicious Cyber Regulation: Balancing the course

Cisco is confident that the current Inquiry will repeat past inquiries performances and provide a path for sustainable and innovative growth.

We welcome any questions you may have and look forward to the opportunity to engage directly with the Inquiry to assist with your goals.