Amstelveen

Amstelveen Pty Ltd
ABN: 54 615 045 531
Level 1, 204 Clarence St
Sydney NSW 2000

18 May 2018

General Manager, Policy Development
Policy and Advice Division
Australian Prudential Regulation Authority
Level 12, 1 Martin Place
Sydney NSW 2000

By email: PolicyDevelopment@apra.gov.au

Dear General Manager for Policy Development,

Re: Consultation on CPS 234 Information Security requirements for all APRA-regulated entities

Amstelveen welcomes the opportunity to respond to APRA's consultation on Information Security requirements for all APRA regulated entities (CPS 234). We are a specialist consultancy which works on major technology and business change projects, and enhances capability in risk management, internal audit and corporate governance functions. We work with some of Australia's largest public and private organisations, including a number of major Authorised Deposit-Taking Institutions (ADIs), insurers, and wealth managers.

We understand that APRA's overall purpose in introducing an Information Security standard is to ensure that relevant entities are aware of new and changing information security threats, and taking appropriate actions to mitigate them. We have reviewed the draft standard and have provided feedback across four key themes:

1. Control management and governance requirements should reflect the unique nature of information security controls;
2. Control testing and asset identification requirements should be clarified;
3. Requirements for incident reporting should be modified; and
4. Stronger emphasis should be placed on non-technical controls.

Within these four themes we have identified a number of observations and recommendations, which we have outlined in this letter.

Overview

Amstelveen supports APRA's move to clarify its information security expectations. This reflects our belief that information security should be a top priority for regulated organisations.

Many larger organisations will not be heavily affected by the new standard due to their level of existing maturity and prior investment in cyber security capabilities. However, for smaller organisations, we believe that this change will have a significant impact and will require considerable effort to implement.

We note that the proposed standard is more comprehensive than comparable industry standards introduced by financial system regulators and governments overseas. The new standard demonstrates APRA's expectation that entities take a holistic approach to information security and have a robust capability in place. This goes beyond the scope of existing local and international regulations, which are primarily focused on the protection of customer and financial statement data. However, the depth of such regulation needs to be balanced with the practicalities and burden of compliance. As such, we have outlined several considerations to help with achieving the right balance.

We also note that the proposed standard does not attempt to specify the controls that entities are required to implement, but rather leaves this to the entities to determine as appropriate. This is a sensible approach given that the threat landscape is continually evolving and that controls need to be suitably adapted. However, there is a risk that entities with a low maturity in information security will fail to adopt the right mix of controls. A robust information security capability is based on a multi-layer approach to security controls that considers a variety of control types, including both preventative and detective controls, and a combination of administrative, technical and physical controls. A number of our recommendations reflect our view that more emphasis is needed in this area, without attempting to dictate specific technical controls.

Detailed Recommendations

1. Control management and governance requirements should reflect the unique nature of information security controls

Currently the draft standard does not directly address the distinction between different information security control types and their placement. Information security controls are typically described as physical, technical or administrative. They may be centrally placed and leveraged across many information assets or unique in nature to a specific asset. Examples of leveraged controls could include, for example, perimeter firewalls, web proxies, data centre security, e-mail security, etc. Controls that are unique to an asset may include system access restrictions, access logs, document encryption, etc. There is a complex interplay between control types and placement of controls, which work together in a multi-layered control environment, or 'defence-in-depth'. This complexity makes meeting APRA's requirements for accountability, escalation and notification challenging.

1.1. Control ownership and accountability

For any given information asset there could be dozens of controls that apply to it. Some of these are unique controls and are typically the responsibility of the information asset owner. Others are inherent in the organisation's environment and have central ownership (i.e. leveraged controls). This distinction, and the need to establish accountability for ownership, is not addressed by the standard.

Recommendation:

- Provide guidance and/or additional requirements in the "roles and responsibilities" section of the standard, covering the need to identify control owners. Entities should identify control owners for leveraged controls, who are accountable for ensuring that the controls are fit-for-purpose. They should also identify owners of information assets, who are accountable for implementing additional unique controls at an asset level where deemed necessary.

1.2. Escalating control deficiencies to the Board

The requirement to "escalate and report to the Board or senior management any testing results that identify information security control deficiencies that cannot be remediated in a timely manner" (s28) is not well

defined. It is also impractical for several reasons:

- Not every control deficiency presents a material residual risk, as there are typically many compensating controls in place as a result of the layered nature of security controls;
- It is not clear what is defined as timely; and
- The volume of control deficiencies reported could be unmanageable and difficult to govern effectively. Any given information asset may have dozens of applicable security controls, and a large organisation can have hundreds or even thousands of sensitive information assets.

Instead trends, themes, and systemic weaknesses in leveraged controls would be more appropriate for escalation. This is an approach which is consistent with the Governance recommendations in the *Prudential Inquiry into the Commonwealth Bank of Australia* report, commissioned by APRA and finalised in April 2018.

Recommendation:

- Revise the requirement to escalate every control deficiency, to require it only in cases where there are deficiencies in key controls or testing indicates systemic weaknesses in controls.
- Provide a clear definition for the meaning of timely, or alternatively remove the timeliness requirement.

1.3. Notifying APRA of material control weaknesses

The draft standard specifies that entities must "notify APRA as soon as possible and no later than five business days after identifying a material information security control weakness which the entity expects it will not be able to remediate in a timely manner" (s35). Materiality is difficult to judge due to the factors outlined above, however it is noted in the discussion paper that "APRA will provide examples in guidance as to the underlying expectations of this requirement."

Based on our experience working with organisations to perform control testing and remediation activities, the five business day requirement may be unreasonable. Often it can take weeks or even months to validate weaknesses after they have been identified and to determine remediation options. Sometimes, this process may include working with third party providers to understand and scope remediation options.

Recommendation:

- Materiality guidance is welcomed; APRA should address the factors outlined earlier with respect to control types and control placement when providing guidance. Some example scenarios of weaknesses that could be useful in achieving APRA's objective could include:
  - Systemic control weaknesses, e.g. if an entity assessed user access lifecycle management as ineffective across the majority of systems; and
  - Instances where there are no effective controls in place against a given threat scenario, e.g. the entity has no controls in place to protect against a Distributed Denial of Service attack.
- Provide a clear definition for the meaning of timely as part of the guidance being developed.
- Consider allowing additional time for entities to notify APRA of control weaknesses, due to their complexity and the time required to validate findings from control testing activities.

2. Control testing and asset identification requirements should be clarified

The distinction between control testing and internal audit control assurance is not clear in the standard and these appear to overlap. Without clarity of APRA's intention, and the meaning of "functional independence", entities may struggle to understand and comply with the requirements. Similarly, the scope of information asset identification and classification requirements needs clarity to make compliance practical.

2.1. Duplicate control testing

The draft standard includes the requirement for an entity to "test the effectiveness of its information security controls through a systematic testing program" (s26) and that "testing must be conducted by appropriately skilled and functionally independent specialists" (s29). It is unclear from whom these specialists should be functionally independent. For example, executive management, asset owners, system users, control owners, etc.

Separately, the standard also mandates that "internal audit activities must include a review of the design and operating effectiveness of information security controls" (s31). It is unclear whether APRA requires that entities perform control testing and control assurance as part of two distinctly separate activities or whether a comprehensive internal audit program of security control testing is sufficient to satisfy both requirements.

Many large regulated entities already have dedicated information security teams performing control testing programs in the first or second line of defence as part of their risk management framework. Typically, internal audit provide assurance that the control testing program is in place and appropriate, often through sample testing, rather than by re-performing testing or creating a duplicate control testing program. This seems to be APRA's suggested approach historically, in *Prudential Practice Guide CPG 234 – Management of Information Security Risk in Information and Information Technology* (s83). However, for smaller entities, this may be an impractical suggestion, especially where implementation of the three line of defence model is less mature and control testing is primarily conducted by internal audit.

Recommendation:

- Clarify whether the requirement for a "systematic testing program" can be achieved as part of internal audit activities. If not, it would be sensible to provide additional guidance as to how the requirements can be satisfied without duplication of control testing activities. Additionally, APRA should clarify the "functionally independent" requirement.

2.2. Information asset identification and classification

The requirement for entities to identify and classify information assets, and to implement controls commensurate with their classification, is a welcome addition, as it is recognised as a critical component of any robust information security management system. However, if the requirement is interpreted in its strictest sense, this will be unachievable for many large regulated entities due to the complexity of their IT environments and the scale of data stored and processed. As defined in the standard, an information asset is "information and information technology, including software, hardware and data (both soft and hard copy)."

Considering hardware alone, it is not uncommon for a large organisation to have hundreds of thousands of individual technology devices, such as laptop PCs, desktop PCs, mobile phones, tablets, servers, network devices, ambient sensors, physical security equipment and more. Just the identification of every hardware asset is challenging, so classifying criticality and sensitivity for each of them as well as every software and data asset would be an enormous undertaking. We are aware of many large organisations that have attempted information asset discovery and classification programs in the past, and failed due to the enormity of the challenge, accuracy of disparate asset data sources and the constantly shifting nature of IT environments. While it is true that security is only as strong as the weakest link, the vast majority of information assets in most organisations pose little risk in isolation. There are typically leveraged (centralised) controls in place that apply regardless of asset classification, such as staff background screening, network perimeter security and building access restrictions.

The discussion paper appears to acknowledge this challenge and states that the "draft CPS 234 does not prescribe the information asset classification method and granularity, leaving the entity to determine the appropriate scaling." However, in its current state the standard makes no provision for this scaling and instead

mandates that an entity "must classify its information assets, including those managed by related parties and third parties, by criticality and sensitivity." It may be sensible to revise this, requiring entities to maintain an information classification framework and process that is applied to assets where deemed appropriate.

Recommendation:

- Require entities to have in place a framework and process for classifying information security assets, and allow entities to set the scope of assets that they apply this to. This will make compliance more readily feasible than a blanket requirement to classify each and every asset.

3. Requirements for incident reporting should be modified

Incident management has a dedicated section in the standard, which is sensible. However, the purpose of notification is unclear and compliance with the requirements will be difficult. An opportunity exists for APRA to use this data to strengthen industrywide cyber security capability, by centrally identifying emerging vulnerabilities and threats, based on reported incident data.

3.1. Scope of incident reporting

The draft guidelines covering the type of incidents that should be reported are broad and open to interpretation. Currently it is stated that the requirement applies to incidents that "materially affected, or had the potential to materially affect, financially or non-financially, the entity or the interests of depositors, policyholders, beneficiaries, or other customers" (s34a).

The standard does not provide clarity on what constitutes non-financial impacts or materiality more generally, although we recognise that APRA has a stated intention to revise the *Prudential Practice Guide CPG 234* with this guidance. Overall, APRA's intent behind incident notifications is unclear, which will make it challenging for regulated institutions to assess the suitability of incidents to be reported. Entities can experience dozens of largely innocuous security incidents every day; without clear guidelines this has the potential to distract management from managing and addressing incidents.

Institutions could also find it difficult to accurately identify "potential" material incidents, as it is difficult to assess avoided impacts of security breaches. For example, an individual bypassing building security gates to obtain unauthorised access to a restricted area has the potential to cause a major security breach, but it is difficult to know if that was actually their intent. In addition, many major cyber security incidents are not targeted attacks but rather general exploits, such as WannaCry, NotPetya, and Spectre/Meltdown, for which it is difficult to assess impact at the time of discovery.

Recommendation:

- Clarify the intended purpose of APRA notification of incidents, and provide materiality guidelines to assist regulated institutions to assess suitability of incidents to be reported.
- Reconsider the requirement to report incidents with "potential" material impacts, given the difficulties in assessing the unrealised impact of security incidents and breaches.

3.2. Timing of incident reporting

The standard requires that APRA be notified "as soon as possible, and no later than 24 hours, after experiencing an information security incident" (s34). This phrase should be refined, as incidents and breaches can often take longer than 24 hours to identify and assess after they have been experienced. For example, in the case of advanced persistent threats, data can be exfiltrated over an extended period of time before the organisation becomes aware of it.

Recommendation:

- Consider revising the requirement to apply to incidents once 'identified' rather than "experienced".
- Consider allowing subsequent analysis of the root cause and impact to be provided at a time thereafter.

3.3. Use of incident data for intelligence sharing

The cyber threat environment is dynamic, with new threats constantly emerging. Currently, mature cyber security functions share intelligence with peers and government agencies through both formal and informal channels. Information can include very detailed and specific threat information (such as IP addresses engaged in malicious purposes) as well as general threat trends and themes. This information provides an opportunity for cyber security functions to anticipate vulnerabilities and threats and to be proactive in defending against them.

As discussed above, it is not clear what APRA's intent is behind receiving incident notifications. However, there is an opportunity to use this incident data to provide intelligence back to the industry. Each entity could use this intelligence to continuously adjust and strengthen their security environment with real-time information from external threats affecting industry peers.

Recommendation:

- Consider establishing an information sharing platform, or working with a government partner such as the Australian Cyber Security Centre, to share insights on emerging vulnerabilities and threats, and to provide intelligence back to the industry based on reported incident data.

4. Stronger emphasis should be placed on non-technical controls

We have identified two areas that warrant a stronger focus in both the new standard and the *Prudential Practice Guide*; information security policy management, and the use of non-technical controls such as training and awareness.

4.1. Information security policy management

The standard requires that entities have in place an information security policy framework (s17), however there is no clear definition of the expectations for this policy beyond that it is "commensurate with [the entity's] exposures to vulnerabilities and threats". No references are made to the policy framework elsewhere in the standard. In our experience, it is common that organisations have aspirational information security policies that are poorly monitored, infrequently updated and not consistently enforced. As a result, the control environment, control testing activities, roles and responsibilities, and other elements of the operating environment are often misaligned with what is documented and agreed in formal security policies.

Recommendation:

- Additional requirements may be necessary to ensure that entities have an appropriate and effective approach to information security policy management. In particular, we recommend that this includes the regular review and update of policies, as well as having processes in place for the ongoing enforcement and monitoring of policy compliance.
- APRA's broad use of the term "information security policy framework" to mean "the totality of policies, standards, guidelines and procedures" appears to align with the industry concept of an Information Security Management System (ISMS). APRA may consider explicitly requiring that entities have in place an information security policy framework that is aligned to industry standards, such as ISO 27001. Requiring alignment with ISMS standards will ensure that each entity's policy framework is dynamic and holistic in nature, and applied effectively across the organisation.

4.2. Non-technical controls

The human element of an organisation's control environment serves both as the strongest defence and greatest weakness. The last few years have seen a rise of security threats resulting from poor information security awareness, weak organisational culture and general human weaknesses exploited through social engineering, such as phishing attacks and pretexting. Numerous research papers highlight that phishing attacks are the primary mechanism for infiltrating organisations. For example, Symantec's *2018 Internet Security Threat Report* identified that 71% of targeted attacks used spear phishing[1].

Examples of high profile security incidents which exploited social engineering include the following:

- In 2011, RSA Security had approximately 40m employee records stolen as a result of phishing attacks against employees.
- In 2014, the personal data of over 145m eBay customers was stolen. Hackers are suspected to have used social engineering to compromise employee credentials.
- In 2015, Anthem, the second largest health insurer in the US, suffered a breach of over 78.8m customer details as a result of a single employee clicking a link in a phishing e-mail.
- In 2015, Ubiquiti Networks Inc, a network technology service provider, lost $46.7m as a result of an attacker impersonating an employee and making fraudulent payment requests to the Company's finance department.

Strengthening the human elements of an information security management system starts with embedding a culture of accountability for managing security risk. Organisations that do this well tend to execute a comprehensive security awareness campaign to ensure that staff understand the importance of managing information security. This is usually supplemented with training, particularly as part of on-boarding activities, that provide the tools, tips and resources to manage information security. As with any other control, these should be subject to control testing such as through internal phishing simulation tests and culture assessments.

Currently, the draft standard and discussion paper does not highlight the need for non-technical controls, such as information security training and awareness, for managing information security. There is a risk that entities do not place appropriate emphasis on these. The existing *Prudential Practice Guide* dedicates a section to this consideration, however there is an opportunity to enhance this through inclusion in the new standard and revision of the practice guide.

Recommendation:

- Consider revising the new prudential standard to make the distinction between technical and non-technical controls, and requiring that entities have an appropriate mix of both. Alternatively, consider requiring that entities have an information security awareness program in place.

[1] *Internet Security Threat Report (Volume 23)*, Symantec, March 2018

Conclusion

We hope that the identified considerations are useful to APRA in the design of the new prudential standard. We would welcome the opportunity to discuss these in further detail at any time in the future.

Sincerely,

David van Gogh
Director

Andrew Millward
Senior Manager

Chris Tran
Consultant

Amstelveen

Amstelveen Pty Ltd
ABN: 54 615 045 531
Level 1, 204 Clarence Street
Sydney NSW 2000
http://www.amstelveen.com.au