INFORMATION PAPER

2015/16 Cyber Security Survey Results

September 2016

Disclaimer and Copyright

While APRA endeavours to ensure the quality of this publication, it does not accept any responsibility for the accuracy, completeness or currency of the material included in this publication and will not be liable for any loss or damage arising out of any use of, or reliance on, this publication.

Contents

Glossary

ACSC	The Australian Cyber Security Centre (ACSC) brings cyber security capabilities from across the Australian Government together into a single location. It is the hub for private and public sector collaboration and information sharing to combat cyber security threats
APTs	Advanced persistent threats (APTs) are characterised as a set of sophisticated, covert and continuous computer hacking processes coordinated by an individual, group and/or nation-state targeting a specific entity. An APT usually targets organisations and/or nations for commercial or political motives. APT processes require a high degree of covertness and diligence over a long period of time (months)
Attack surface	Attack surface is a measure of the number of points or avenues where an attacker can attempt to compromise security
AusCERT	AusCERT is a leading Cyber Emergency Response Team for Australia and provides information security advice to its members, including the higher education sector. AusCERT is a single point of contact for dealing with cyber security incidents affecting or involving member networks
Cyber attack	The use of computer-based technology to compromise confidentiality, integrity or availability of IT assets. This may be done to achieve a range of objectives (e.g. financial gain; political/social change; intelligence gathering; or warfare)
Cyber security	Refers to measures aimed at protecting systems and data from cyber attacks
DoS / DDoS	A denial of service (DoS) attack is a technique used whereby digital services (internet or mobile) are overwhelmed with fake requests, preventing legitimate access by customers/business partners. A distributed denial-of-service (DDoS) is where the attack source is distributed over a large number of locations across the internet, making it more difficult to filter attack requests from legitimate requests
IT assets	IT assets refer to software, hardware and data/information (both soft and hard copy)
Malware	Malware (malicious software) refers to a family of software that can be used to disrupt or gain access to systems, gather sensitive information or execute unauthorised functions
Phishing, spear phishing	Phishing refers to impersonating a trusted entity in an electronic communication in order to attain sensitive information such as usernames/passwords or credit card details. Spear phishing is phishing tailored for specific individuals or companies in order to increase the likelihood of success
Ransomware	A ransomware attack occurs when malicious software infiltrates a device or network and proceeds to encrypt data on local and network drives, rendering them unreadable. A ransom message and payment instructions are then displayed by the software to facilitate payment in exchange for the decryption of the data

Introduction

Cyber attacks are increasing in frequency, sophistication and impact, with perpetrators continuously refining their efforts to compromise systems, networks and information world-wide. The financial sector is one of the more prominent targets for such attacks, and recent incidents involving financial institutions in Bangladesh, Vietnam, South Africa, Japan and Ecuador demonstrate the absence of geographic constraints in cyberspace.

Financial institutions are investing considerable effort and expense to protect their IT assets. However, in parallel, many APRA regulated entities are also adopting strategies which will see more data stored and/or processed outside the perimeters of the regulated entity. In addition, entities are increasingly granting service providers access to their environments to perform business and technology processes.

Inherently these trends expand the attack surface for cyber adversaries to exploit, suggesting that the frequency and potential impact of cyber security incidents will continue to increase.

As part of its activities to understand and assess industry preparedness for, and resilience to, cyber attacks, APRA undertook a survey between October 2015 and March 2016 to gather information on cyber security incidents and their management within APRA-regulated sectors.

Respondents to the survey included 37 regulated entities and four significant service providers, covering all APRA-regulated industries, with the exception of private health insurance. The results of the survey will guide APRA's supervisory activities in this area and inform updates to relevant prudential requirements and guidance. Regulated entities will also be able to compare the survey results with their own experiences and assess their level of cyber security preparedness.

Survey results analysis

The survey comprised a combination of closed and open questions, aimed at gaining insight into industry-wide issues, practices, challenges and concerns in the area of cyber security including:

- incidents experienced;
- capabilities for prevention, detection and response; and
- approaches to governance, risk management and assurance.

The representative sample of the entities surveyed, breadth of questions involved and overall quality of responses provided suggest that the conclusions from the survey have wide-spread validity.

The survey results, in conjunction with other supervisory information, confirm that APRA-regulated entities, not only the largest of these entities, need to operate on the assumption that cyber attacks will occur and that such attacks will remain a constant challenge. Furthermore, it would be prudent for these entities to operate on the assumption that cyber attacks will become both more frequent and more sophisticated over time.

Incidents

Surveyed entities experienced a range of cyber security incidents during the 12 months prior to the APRA survey that varied in nature, sophistication and impact. The cyber threats that had the potential to cause a material impact appear to have been well managed through a combination of effective monitoring and response activities, often supplemented by the use of external expertise.

Just over half of all survey respondents - 20 regulated entities and one service provider - experienced at least one cyber security incident in the 12 months leading up to the survey that was sufficiently material to warrant executive management involvement.

Types of Incidents

The incidents reported highlight the evolving range of threats and the importance of diligence in maintaining defences commensurate with the threat landscape. Incidents reported by survey respondents included:

- potentially high impact incidents such as advanced persistent threats (APTs), distributed denial of service (DDoS) attacks and compromises of highly privileged access. These were experienced by a number of respondents (21 per cent) and reinforce the value of preparedness (prevention, detection and response controls) in the face of sophisticated attacks which cannot always be prevented;
- ransomware attacks, which represent an increasing threat. The reported incidence of these attacks (14 per cent of respondents) reinforces the importance of frequent system and data back-ups as a last resort mitigation;

- potentially reputation damaging incidents such as website defacement and social media account misuse, which were experienced by approximately 1 in 8 entities (12 per cent of respondents). Whilst these incidents have had a low impact and frequency to date, the potential reputational impact necessitates continued vigilance with respect to the management of public facing channels and services; and
- other incidents with low impact such as compromise of client accounts, internet banking fraud, phishing and malware attacks. These were experienced by almost 1 in 4 respondents (24 per cent).

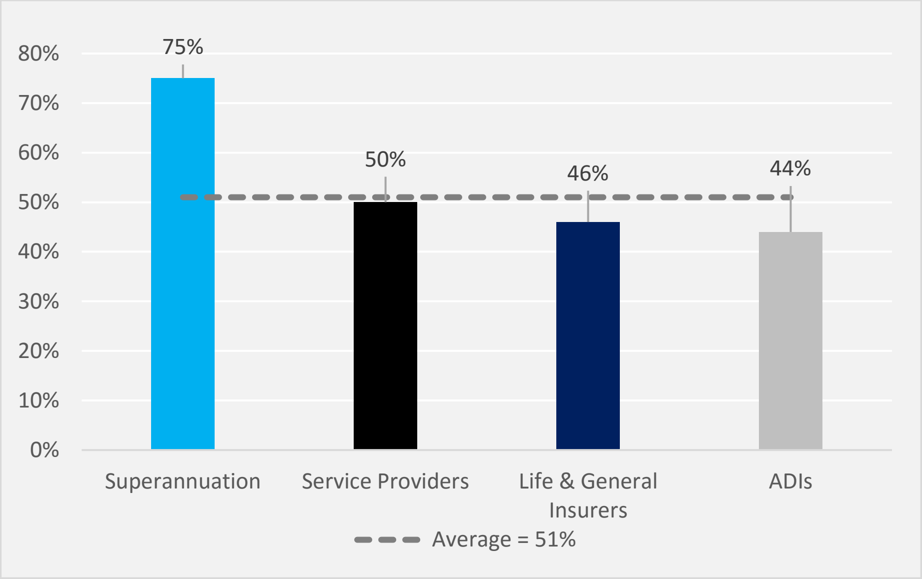
Figure 1: Common cyber attack methods as identified by survey respondents

Malicious software	Worms, viruses, trojans, backdoors, logic bombs, rootkits, ransomware
Spyware	Key loggers, screen scrapers
Denial of service	Denial of service attack
Computer takeover	Rootkit
Malicious computing network	Botnets, denial of service as a service, spam as a service
Social engineering	Spam, phishing, spear phishing, whaling
Vulnerability	Exploits, including zero-day exploits

Frequency of significant cyber security incidents by Industry

Superannuation industry respondents reported a higher occurrence of incidents that warranted reporting to executive management as compared to other industries (refer to Chart A). While the underlying cause of this was not apparent in the survey results, possible explanations are that the superannuation industry is a more attractive target to perpetrators due to the relatively high customer account balances, and/or variances in reporting thresholds between the industries.

Chart A – Occurrence of cyber security incidents by Industry

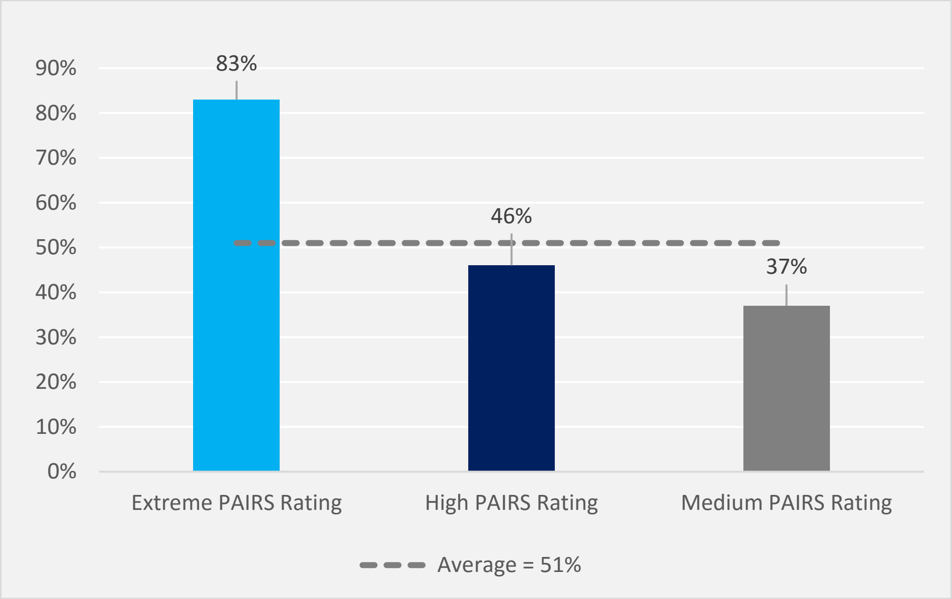


Percentage of respondents by industry group that experienced a cyber security incident in the past 12 months sufficiently material to warrant reporting to executive management.

Frequency of significant cyber security incidents by entity size

It was observed that the frequency of incidents directly correlates with entity size (as measured by APRA's PAIRS impact rating[1]) where the group of the largest regulated entities experienced almost twice as many significant cyber attacks as compared to the next largest group (refer to Chart B). This result is perhaps unsurprising: larger entities may be more attractive targets due to their visibility and/or the relatively larger attack surface.

Chart B – Frequency of significant cyber security incidents by entity size



Percentage of respondents by size who experienced a cyber security incident in the prior 12 months sufficiently material to report to executive management.

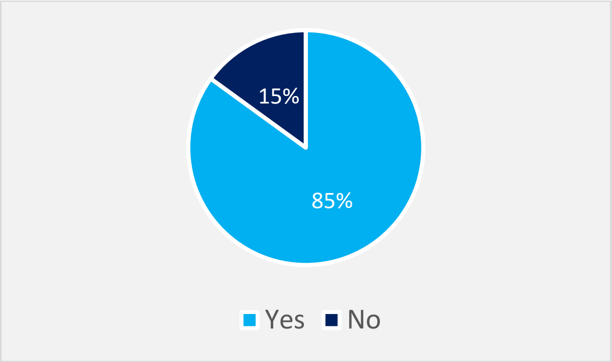
Governance

Information on internal and external incidents and visibility of the entity's capability to prevent, detect and respond to the wide range of possible cyber security incidents is crucial to enable effective governance in this area.

APRA expects Boards and executive management to be well informed so they can effectively discharge their oversight responsibilities and decision making. The survey found that most, but not all, Boards / Board committees and executive management are periodically updated on cyber security matters (refer to Charts C and D). The greater proportion of reporting to Boards over executive management reflects that Trustee Boards act as the primary governance authority for Superannuation funds.

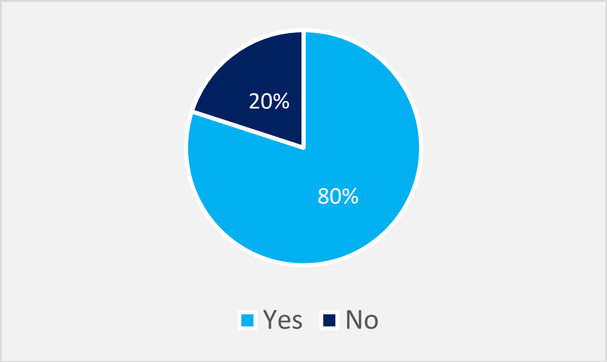
[1] Probability and Impact Rating System (PAIRS) is APRA's risk assessment model. It incorporates two dimensions: the Probability and Impact of the failure of an APRA-regulated entity.

Chart C – Periodic cyber security updates to Board or Board committees



Percentage of respondents who indicated that their Board or Board committees received periodic updates on cyber security.

Chart D – Periodic cyber security updates to executive or executive committees



Percentage of respondents who indicated that their executive or executive committees received periodic updates on cyber security.

For those respondents which had provided periodic updates to Board members and executive management, the survey identified some shortcomings in coverage, with certain topics less commonly reported than expected. Specifically, cyber security incidents experienced (internal and external); the results of relevant assurance activities (internal and service provider environments); security strategy; and the results of cyber security scenario testing.

It is important that Board and executive management are well-informed regarding cyber security risks and their organisation's preparedness to prevent, detect and respond. Figure 2 represents a composite of information commonly provided to Boards / Board Committees and executive management teams by survey respondents. The list below can be used to assist entities in assessing the completeness of their current reporting mechanisms.

Figure 2: Common information reported to Board members and executive management

Security strategy	Security capability self-assessment
Informational and educational material	Assessment of third party security
Security incidents	Cyber security capability benchmarking
Existing security risks	Assurance results
Emerging security risks	Penetration test results
Security risk mitigation strategies and plans	Results of cyber-simulation activities
Implementation of specific security controls	Results of training and awareness sessions
Results of security control effectiveness assessment	Assessment of effectiveness of brand protection controls in the online space

Risk & Assurance

APRA expects regulated entities to fully understand the key risks facing their organisation, the nature of any deficiencies in the controls that mitigate key risks and progress of deficiency remediation.

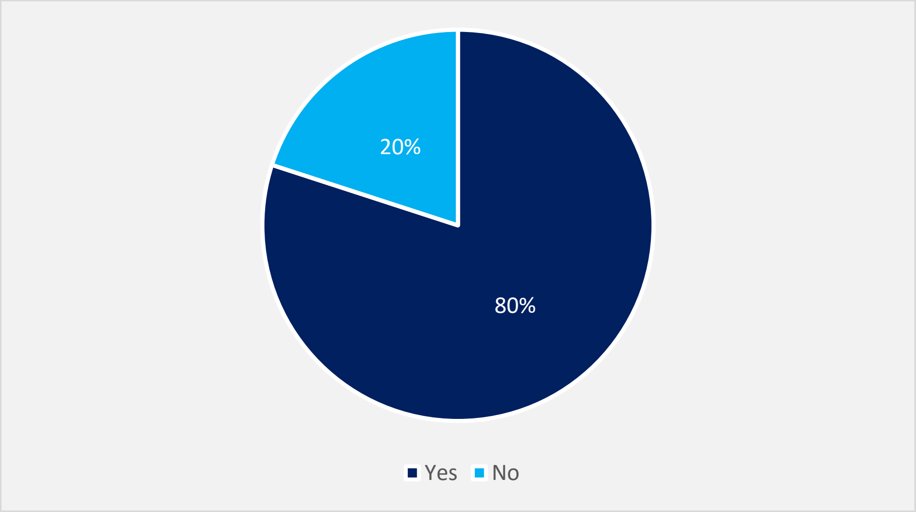
All bar one of the survey respondents identified cyber security scenarios under their Risk Management Framework (RMF) and most survey respondents identified cyber-related risks as one of their top enterprise risks (87 per cent of respondents). There was a wide range in the quality and quantity of scenarios identified. Some entities only identified a limited number of scenarios (much fewer than commonly observed), while some others cited quite generic scenarios which would be hard to use to inform specific incident response plans. Only one entity specifically identified an APT attack as a scenario; the same entity had suffered two such incidents. A few entities, however, were more comprehensive in this area and identified a range of specific scenarios (refer to Figure 3).

Figure 3: Common scenarios identified by respondents for cyber security risk management

Compromise of a service provider to facilitate cyber attack(s)	Inappropriate or elevated system access
Compromise of data and/or systems by staff / contractor	Physical attack against multiple data centres
Disclosure of large sets of confidential data (customer and/or internal)	Social engineering attacks against staff and/or customers (e.g. phishing and spear phishing)
Exfiltration of intellectual property and/or market sensitive data for strategic, commercial, or political gain	Social media brand attack to cause large scale reputational damage
Exploit of poorly designed applications / code	Systems not adequately configured and/or patched against security weaknesses
Extensive virus / malware / ransomware attack	Targeted, advanced and persistent attack by nation state or other group
High value cyber-crime / fraud against customers or systems	

Independent assurance is an important discipline for assessing cyber security preparedness. Four out of five survey respondents had cyber security related findings that warranted action. Findings identified included a broad range of issues across prevention, detection and response controls. Entities should be mindful to assess the severity of the findings using their own operational risk framework in order to appropriately represent the risk exposure, as opposed to relying solely on the service providers' ratings.

Chart E – Prevalence of cyber security findings from independent assurance



Percentage of respondents who had cyber security related findings identified that warranted action

Regulated entities need to ensure they have a complete view of their organisation's capability to prevent, detect and respond to cyber-attacks. Given their increasingly important role in day-to-day operations, this view must include key service providers.

The survey also found that assurance over service providers' cyber security capabilities varied in comprehensiveness. Larger entities tended to have outsourcing management frameworks which comprise a range of assurance mechanisms, including on-site assessments. Examples of other practices reported by survey respondents included reliance on other reviews (e.g. external audit, penetration tests); certifications; provider self-assessments; contractual/service level agreements; on-boarding due diligence; and pre-approved panellists.

Capabilities

Regulated entities have recognised and acted upon the need to use external expertise to address skill and capability gaps. All survey respondents, bar one, indicated they have cyber security capability improvement plans in place. The improvements planned typically relate to implementations of Security Incident and Event Monitoring (SIEM) systems, intrusion prevention and detection systems (IPS/IDS), transitions to managed security services arrangements, implementation of encryption and data loss prevention (DLP) technologies.

The vast majority of survey respondents have engaged a specialist security services provider (93 per cent of respondents). This is predominantly to conduct security penetration and vulnerability assessments, but also includes managed security services (i.e. outsourcing of maintenance and security monitoring of the IT environment). A very small number of entities also use external expertise to conduct architecture and solution design reviews and maturity benchmarking exercises (7 per cent of respondents). Figure 4 lists common use cases for external cyber security specialists as reported by survey respondents.

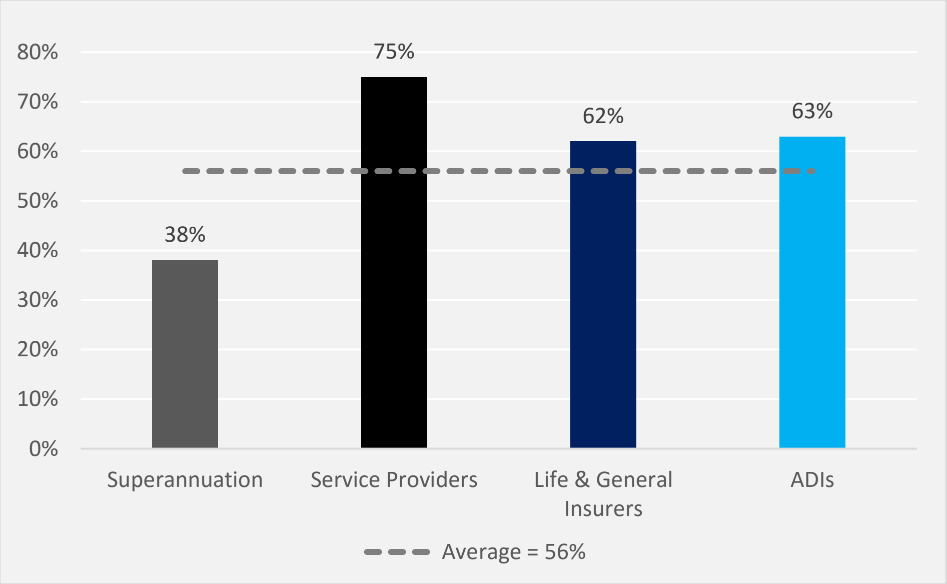
Figure 4: Common use cases for external cyber security specialists

Architecture review and advice	Cyber security insurance providers
Business continuity and disaster recovery advice	Security Operations Centres (SOCs)
Anti-DDoS solutions	Security assurance testing (e.g. penetration tests)
Cyber forensic and data breach specialists	Threat intelligence feeds

The use of third parties to ensure access to appropriately-skilled resources is pragmatic and sensible, particularly in an area where it is increasingly difficult to maintain an effective internal capability, especially for smaller entities. However, this increases the need for effective management and oversight of outsourced arrangements.

The majority of survey respondents have tested their ability to respond to and recover from cyber security incidents during the survey period (56 per cent of respondents - refer to Chart F). Given the nature and frequency of cyber security incidents, there is growing recognition within industry for the need to regularly test response and recovery capabilities for a range of cyber security scenarios. Incident response testing will also be an area of increased supervisory focus.

Chart F – Testing of cyber security capabilities by industry



Percentage of respondents by industry group who indicated that they have tested their ability to respond and recover to cyber security incidents.

The majority of survey respondents have established links with Government agencies in relation to cyber security (69 per cent of respondents). CERT Australia and Australian Federal Police were the most frequently mentioned agencies. Engagement with these agencies is important as a source of threat intelligence and assistance in responding to certain types of cyber security incidents. All regulated entities should consider establishing links with the Australian Cyber Security Centre (ACSC) if they have not already done so.

It is important for regulated entities and service providers to improve cyber security capabilities through collaboration by engaging with relevant forums and other sources of threat intelligence and response assistance. Figure 5 summarises common forums and sources used by survey respondents, and can be used to assist entities in assessing the completeness of their current engagements.

Figure 5: Common forums/sources of threat intelligence and response assistance

AusCERT	Customer Owned Banking Association (COBA) forums
Australian Information Security Association (AISA)	Financial Services-Information Sharing and Analysis Center (FS-ISAC)
Australian Institute of Superannuation Trustees (AIST) security forums	ISACA events
Australian Interbank Forum	National Intelligence Exchange (NIE)
Australian Mutual Security Committee	Security consultancy forums
Australian Signals Directorate OnSecure website	Security vendor conferences
CERT Australia	Trusted Information Sharing Network (TISN) for Critical Infrastructure Resilience
Cloud Security Alliance	

Opportunities for improvement

While the incidents experienced by the survey respondents appear to have been managed effectively, areas for improvement were also identified. In particular, the survey results, and recent supervisory activities, were useful for identifying a set of practices that would benefit all regulated entities. These practices are summarised in Figure 6 and should be considered by all regulated entities in their strategic and tactical planning to improve cyber security risk management.

Figure 6: Practices for sound cyber security risk management

Governance	Ensure boards and executive management are well informed regarding cyber security risks and their organisation's preparedness to prevent, detect and respond.
Preparedness	Regularly test response plans for common cyber security incident types, including verified recovery capability for plausible worst-case scenarios.
Scope	Cover the extended enterprise, including service providers, joint ventures and offshore locations when scoping cyber security risk management activities.
Strategy & funding	Maintain a rolling strategy to address the evolving forms of cyber security risk, supported by ongoing investment.
Capabilities & resourcing	Maintain sufficient access to specialist cyber security resources (either internally and/or via establishing partnerships).
Situational awareness	Establish threat intelligence and other information sources on the latest attack vectors and countermeasures which are used to inform security practices, including monitoring and subsequent response.
Incident response	Adopt an 'assumed breach' mentality and invest in capability to detect and respond to cyber security incidents in a timely manner.
Assurance	Maintain ongoing assurance over effectiveness of prevention, detection and response capabilities.
Collaboration	Share threat and response information with Government, industry and customers to improve prevention, detection and response capabilities.

Concluding remarks

Cyber security threats continue to evolve. Given the observed frequency of significant cyber security incidents, the range of threats and the prevalence of high risk cyber security findings, it is important that all regulated entities have an ongoing strategy to address the evolving forms of cyber risk. This includes ongoing investment in cyber security capabilities and effective management and oversight of the extended enterprise, including service providers and offshore locations.

Preparation for cyber security incidents is vital. In addition to periodic assessment of the adequacy of prevention and detection controls, regulated entities should test their cyber security response and recovery capabilities on a regular basis. This may be either as a part of business continuity testing or as a stand-alone activity.

Given that even the largest regulated entities are challenged to maintain and enhance their internal cyber security capabilities, the use of third parties to provide access to specialist resources (prior to, during and after a cyber security incident) may help many entities strengthen their resilience to cyber attack.

Engagement with Government, peers and service providers is also important in this area, particularly in light of the recently launched Australian Cyber Security Strategy and associated plans to improve cyber defence capabilities (including threat intelligence). Early engagement will allow entities to maximise the benefits of these Government-sponsored initiatives.

To date, no APRA regulated entity has suffered material losses from a cyber incident, and security controls have held up against past attacks. However, this should not provide grounds for complacency. As a result of the expanding sophistication, frequency and impact of cyber attacks, APRA-regulated entities should expect to experience significant cyber security incidents and be prepared for an evolving range of threats. APRA intends to lift the supervisory and regulatory expectations for regulated entities to not only secure themselves against cyber attacks, but to implement improved mechanisms to quickly identify and remediate successful attacks when they occur.

Regulated entities therefore need to continue to enhance their prevention, detection and response capabilities, test their preparedness and work collaboratively with peers, researchers and government to improve their level of cyber resilience. There is no ‘finish line’ for cyber security risk management: it is a necessary discipline with no room for complacency, and will require on-going vigilance, improvement, investment and oversight.

APRA