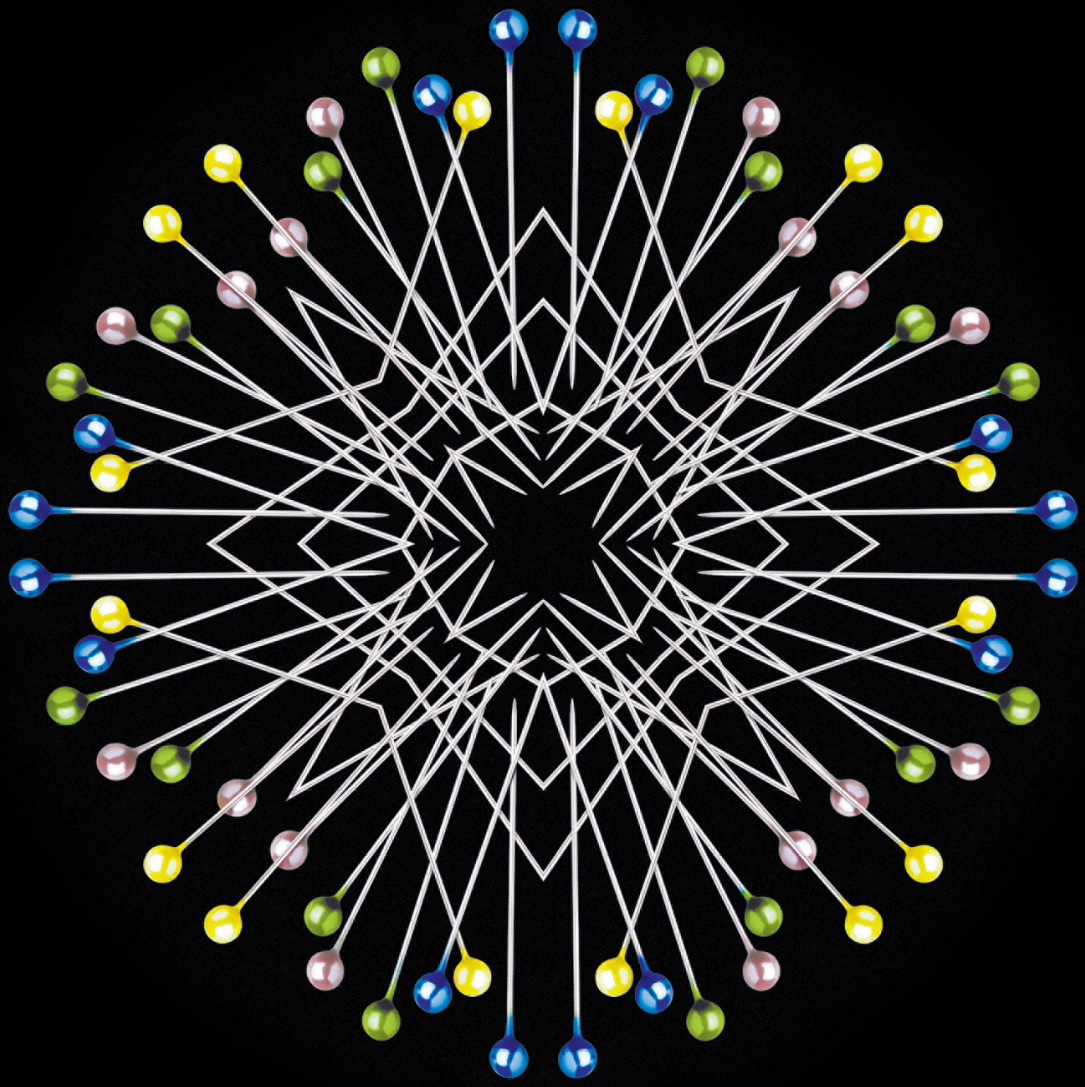
Deloitte.



Cyber regulation in Asia Pacific

How financial institutions can craft a clear strategy in a diverse region

CENTRE *for*
REGULATORY
STRATEGY
ASIA PACIFIC

Contents

Introduction

This paper aims to shed light on regulation emerging in the cyber risk realm for financial institutions (FIs) active in Asia Pacific (APAC) and to help those institutions craft a clear strategy in this diverse region.

First, we provide a framework by which FIs can assess their own cyber risk capability and strategy, and understand the different regulatory approaches.

Then, we give an overview of recent financial services (FS) regulatory developments in regards to cyber risk in seven jurisdictions across the region: India, People's Republic of China (China), Hong Kong Special Administrative Region (Hong Kong), Republic of Korea (Korea), Japan, Singapore and Australia. By laying out these FS regulatory approaches and trends, we hope to assist FIs stay ahead of regulatory developments.

Finally, we recommend practical steps that FIs can take to develop a coherent region-wide cyber risk strategy to minimise regulatory risk.

Although informing elements of cyber risk strategies, this report does not focus on privacy or personal data protection regulation. For an analysis of major privacy and data protection considerations and developments in APAC, please refer to Deloitte's recent publication ***Building trust across cultures: Privacy and data protection***[1]. Similarly, while helping to shape various pieces of cyber policy and regulation, this report does not address laws that concern specific cybercrimes or that primarily seek to address national security, defence and geopolitical issues.

Cyber risk impacts and challenges

Across the globe, and within APAC, cyber-attacks are increasing in frequency and sophistication. It has been estimated that such attacks cost the global economy one per cent of annual GDP[2] and cybercrime up to US$575bn per year[3]. The FS sector is a key target and there are many well publicised cases involving FIs (see figure 1, opposite).

The financial system relies on maintaining the strict confidentiality of data. A cyber attack can cause personal and commercial data to be lost or compromised, and prevent important services from being provided. FIs and their customers can also face significant financial loss from cyber attacks. Cyber risks are only set to grow as FIs become more data-driven digital businesses, and as more financial services are delivered online. Only those FIs who have robust cyber security and cyber risk management will be in a position to retain customers, trust and a competitive edge. As observed by Ashley Alder of the Hong Kong Securities and Futures Commission (SFC), "There is no doubt that cyber security threats are now the top risk for banks and the broader financial system"[4]. Indeed, the International Organisation of Securities Commissions (IOSCO) has called cyber risk "a growing and significant threat to the integrity, efficiency and soundness of financial markets worldwide"[5].

The environment described above has made managing cyber threats a priority for industry, policy makers and regulators. For example, in late 2016 SWIFT announced the introduction of a set of mandatory core security standards and an associated assurance framework for its customers, with inspection, enforcement and reporting of any non-compliant customers to regulators commencing 1 January 2018[7]. While industry driven activity moves forward, regulators are considering appropriate standards and supervisory tools, and are actively urging firms to enhance capabilities.

Challenges for APAC FIs

Cyber security threats are not confined within national borders. The financial system is extensively interconnected and there is increasing information and communications technology interdependence within APAC.

The strength of one FI's cyber security can be heavily influenced by another FI's cyber risk management, as well as that of service providers and other ecosystem members. For example, the international interbank messaging system SWIFT interconnects the majority of banks, such that any weakness in one node would impact others; this means that an FI with poor cyber risk practices could potentially be leveraged to compromise other FIs that may have more secure procedures. Widespread use across FIs of the same software can also mean that hacking into one system will quickly spread into others.

Although cyber threats cut across borders, cyber security regulation in the APAC region remains fractured and localised, with no significant moves toward harmonisation. FIs struggle to understand the regulatory idiosyncrasies at country level, to be cognisant of emerging threats and to design cyber risk programs that are coherent and robust across jurisdictions. The lack of a harmonised and cooperative regulatory environment in part reflects the political, economic and socio-cultural variety in the region, the significantly differing technological capabilities and the geopolitical concerns unique to each nation.

Another challenge for FIs operating in APAC (and indeed across many parts of the globe), is that human resource capabilities are generally lacking.

Organisations have a shortage of dedicated IT security specialists and cyber professionals, which means they may have difficulty staying up to date with the pace of change in the cyber landscape. Cyber risk management frameworks in FIs are also often externally focused and insufficient resources are devoted to internal control. Many FIs lack management recognition or understanding of the importance of cyber security and fail to adopt a coordinated approach across functions[8].

Overcoming challenges

The regulatory trend in many parts of APAC and amongst supranational regulators is to cyber resilience. This approach accepts the inevitability of cyber-attacks and places emphasis on building holistic, dynamic, enterprise wide cyber risk programs that are continually tested and updated to allow for agility and swift recovery. Strategies that enhance measures in securing perimeters and staying vigilant for emerging threats, that also ensure insights flow through to a resilient cyber ecosystem and that have senior support and oversight will be the cyber risk strategies that best position FI's to stay ahead of regulatory expectations.

Beyond this, industry and regulators should work together to further the development of cyber skills and expertise, to foster common standards and approaches, to support information sharing (across borders, between FIs and between regulators and regulated) and to facilitate coordinated responses to incidents and attacks.

Figure 1: The impact of cyber attacks

Cyber crimes cost
US **$575B**
per year[10]

In 2016 hackers

Withdrew **US$81 million** from the Bangladesh Central bank[11]

Accessed and leaked the details of **3.2 million** customer cards from several Indian banks[12]

Stole **US$65 million** of bitcoins from Hong Kong based digital currency exchange Bifinex[13]

Used malware to steal **US$2.17 million** from eight banks in Taiwan[14]

In 2017

Korea's **seven main banks** were threatened with a distributed denial of service attacks should they fail to pay a ransom[15].

A framework for assessing approaches to cyber risk

Regulatory and FI approaches to cyber risk can be examined against the Deloitte Global Cyber Strategy Framework, which is summarised in Figure 2, opposite.

Governance
The Framework identifies that the foundation and starting point for an effective cyber risk management strategy is implementing effective governance. This means ensuring that the necessary structures and rules are in place to maintain and enhance preventative and detective cyber security capabilities.

It ensures that support for, and oversight of, risk management and key decisions on cyber security sit with senior management. It also ensures cyber risk culture is embedded throughout the organisation, and that cyber risk is intrinsically linked to the strategic and business objectives for the organisation.

Strategy
Traditional security programs have often been unsuccessful in unifying the need to both secure and support technology innovation required by the business. Having a cyber strategy supports the transition to an executive-led cyber risk program that balances requirements with the strategic objectives and risk appetite of the organisation in establishing an actionable road-map to support the evolution of security program priorities.

There are also three broad approaches to managing cyber risk identified by the framework:

Secure
Proactive protection against successful cyber-attacks before they occur by developing, implementing, and enhancing the controls that safeguard digital assets.

Vigilant
Ability to discover internal and external threats by leveraging the available threat intelligence, and pro-actively mitigating them or minimising any potential adverse impacts to the organisation.

Resilient
It is not a question of whether an attack will or will not occur, but rather a question of when. Therefore, crisis readiness, incident response and business recovery plans are vital.

Adopting a secure, vigilant and resilient approach, enabled by effective strategy and governance, is key to managing cyber security risk, continued business performance and meeting regulatory expectations.

Figure 2: The Deloitte Global Cyber Strategy Framework

Strategy

- Cyber strategy, transformation, and assessments
- Cyber risk management and compliance
- Cyber training, education and awareness.

Secure

- Infrastructure protection
- Vulnerability management
- Application protection
- Identity and access management
- Information privacy and protection.

Vigilance

- Advanced threat readiness and preparation
- Cyber risk analytics
- Security operations center
- Threat intelligence and analysis.

Resilience

- Cyber incident response
- Cyber wargaming.

Regulatory trends and recent developments

This section explores recent developments and trends in FS cyber security regulation in seven APAC jurisdictions. Focus is placed on regulation administered or developed by FS regulatory agencies, as this is of particular relevance to FIs. Figure 3, opposite, identifies the key FS regulators for the seven APAC jurisdictions covered in this paper.

Regulation is developing across the region, although it is not uniform. As previously noted, regulatory approaches to cyber risk in APAC are varied and localised, with no significant steps taken yet toward harmonised standards across the region. Not surprisingly, economies with different levels of cyber exposure and capacity address the issue differently. Generally, businesses operating in countries that have more advanced ICT infrastructure and a bigger digital economy face greater cyber risks. For example, Korea, Australia, Japan and Singapore have been found to be nine times more vulnerable to cyber-attacks than other Asian economies[16].

Looking through the lens of the Deloitte Global Cyber Strategy Framework, we see the recent focus for FS regulators in Japan, Hong Kong, Singapore and Australia has been to strengthen FIs resilience. Korea is heavily dependent on cyber technology and has been actively amending its sophisticated framework from all dimensions, with a particular focus on controlling sensitive information. China and India have emphased being secure, however, both are now moving toward developing FIs vigilance and resilience.

In relation to secure responses, authorities across the region agree on the importance of strengthening the protection of personal and sensitive information. The defence against outsourcing risk is an emerging and growing area of concern, in particular for those economies where IT services are widely contracted out to jurisdictions with weaker cyber security regimes.

Among the approaches to improve vigilance, facilitating information sharing is the core endeavour of new regulatory proposals. Authorities in the region are calling for increased information sharing both amongst FIs and between FIs and regulators.

As noted, there is a growing trend amongst FS regulators in APAC, and across the globe, to building resilience. The rationale behind the push to building resilience is that in the modern digital economy cyber attacks and data breaches are inevitable and that response readiness is key to a sustainable enterprise. Attention is being placed on conducting attack drills, simulation exercises, and contingency planning. Investing in cyber insurance is similarly being discussed as a tool that firms can enlist to manage their cyber risk and build resilience.

Effective governance is also an important theme for regulators, with particular attention being placed on executive led cyber security strategies and extending management of cyber issues beyond the IT department and into the entire enterprise. Upskilling the workforce and building cyber security expertise is another theme in new FS regulatory initiatives, which also demonstrates a focus on good governance and management throughout the organisation.

In the pages that follow, snapshots are provided of recent FS regulatory developments and trends in the seven jurisdictions covered in this report.

Figure 3: Key financial services regulators in Asia Pacific

Australia

Australian cyber security regulation remains scattered among various pieces of legislation, standards and regulatory guidance documents. Nonetheless, there are moves towards centralisation with 2016 seeing the release of Australia's Cyber Security Strategy[17], as well as the appointments of the first Minister Assisting the Prime Minister on Cyber Security and a new Special Adviser to the Prime Minister on Cyber Security[18].

Recent FS regulatory developments: FS cyber security regulation in Australia is generally principles and risk based, giving FIs the flexibility to determine appropriate strategies[19]. Cyber security is, however, top of mind for Australia's FS regulators. ASIC, Australia's market conduct regulator, has identified cyber resilience as a key long term challenge,[20] "signalling increased regulatory scrutiny of this issue"[21]. APRA, Australia's prudential regulator, has similarly said it intends "to lift the supervisory and regulatory expectations for regulated entities" with regards to cyber security[22].

ASIC Report 429 Cyber Resilience: Health Check

In March 2015, ASIC released Report 429 Cyber Resilience: Health Check to help FIs improve their cyber resilience. Recommendations include: board engagement on cyber risk strategy; proactive policies, which are regularly reviewed and updated; fostering a culture of cyber resilience and incorporating a resilience approach into cyber security frameworks; implementing the Australian Signals Directorate's 'top four' strategies to mitigate cyber intrusions; assessing internal approaches against the NIST Cyber Security Framework and reviewing the cyber risk management practices of vital third-party providers and clients[23].

APRA Information Paper: 2015/16 Cyber Security Survey Results

APRA's September 2016 Information Paper – 2015/16 Cyber Security Survey Results also provides insights into regulatory thinking.

It warns FIs to be careful of complacency, to "operate on the assumption that cyber-attacks will occur and that such attacks will remain a constant challenge" and 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". The paper also lists the practices APRA sees as essential for sound cyber security risk management, such as: ensuring boards and executive management are well informed regarding cyber security risks; regularly testing response plans; having the extended enterprise, including service providers, joint ventures and offshore locations included in cyber security risk management activities; and investing in capabilities to detect and respond to incidents in a timely manner.

ASX 100: Cyber Health Check Report

In April 2017 the Australian Securities Exchange released the ASX 100 Cyber Health Check, the results of a survey of how the boards of Australia's largest publicly listed companies view and manage their exposure to the cyber world[24]. Although an industry-led initiative, the report forms part of the Australian Government's Cyber Security Strategy. It includes a foreword written by the Prime Minister and involved collaboration with government bodies including ASIC and the Department of the Prime Minister and Cabinet. The results of the survey aim to provide "a baseline where companies can see how they rate against their peers and can take practical steps to improve their cyber security".

Cyber security is acknowledged as a major and growing risk. Key trends identified in the report (that will likely be the focus of future industry and regulatory work) include the need for a culture of collaboration and the importance of effectively defining and analysing cyber exposure.

Future trends

Mishandling of data in the outsourcing process is an emerging area of focus for Australian FS regulators. New personal data breach notification legislation was passed in February 2017 that requires serious breaches to be reported to authorities and affected individual(s)[25], the knock on effect of which may be improved information and intelligence sharing and focusing board and senior executive attention on the importance of cyber issues.

People's Republic of China

Chinese authorities place great importance on cyber security. Indeed, President Xi Jinping himself leads the Office of the Central Leading Group for Cyberspace Affairs. Cyber security regulation in China is becoming increasingly centralised and places emphasis on controlling data and sensitive information, including data localisation rules and state approval of technology.

Recent FS regulatory developments:

Cyber Security Law of China

Undoubtedly the most significant recent development has been the passing of the Cyber Security Law of China (CSL) in November 2016. The law, which took effect on 1 June 2017, provides a comprehensive regime for privacy and cyber security regulation in China.

Obligations are imposed on 'critical information infrastructure operators' (CIIs) and 'network operators', and FIs are likely to fall within both categories. Among other things, network operators will need to create cyber security policies and procedures, determine the people responsible for cyber security and create incident contingency plans. CIIs are subject to additional requirements that include having designated cyber personnel, conducting periodic cyber security training, implementing disaster backup processes and conducting annual security assessments. In addition, personal information and important business data collected or generated in China by CIIs must be stored within China (unless necessary to provide to overseas parties, in which case a security assessment will be conducted by the authorities). Reporting incidents to data owners and authorities, as well as assisting the state on national security matters and cybercrime investigations, are other elements of the new regime.

Additional regulations are being proposed to supplement and clarify aspects of the CSL, including Measures for Examining the Security of Network Products and Services (May 2017), Administrative Provisions for Internet News Information Services (May 2017) and the Draft Regulation for the Protection of the Critical Information Infrastructure (July 2017).

Some concerns have been expressed that the CSL will force businesses who operate in China to only use local technology, which may not be best of breed or fully compatible with offshore systems and infrastructure, and will be particularly challenging for organisations that rely on cross-border data transfers. Further guidance is expected from authorities that will hopefully clarify these issues. What is certain is that given the size and importance of the Chinese economy to the wider region (indeed the globe), its cyber regulation will impact the business of many FIs.

Cybersecurity Classified Protection Standards

In order to implement the requirements of CSL, regulators are developing more detailed standards and guidelines in specific industries and technical areas. The new Cyber Security Classified Protection Standards have been in draft for comments since 2016.

The new standards emphasise the protection of personal information and the management of the IT supply chain's security, and further extend to some specific technologies, e.g. the cloud security, mobile internet security and big data security, which are widely used in the financial industry.

Draft Cryptography Law

A draft law on cryptography has recently been released which proposes, among other things, that CIIs comply with relevant national standards, as well as assessments and security reviews of certain cryptography products, services and security systems.

CBRC and CIRC measures

China's banking and insurance regulators have released draft technology risk management guidelines setting out detailed requirements for regulated institutions, which are broadly aligned with the CSL. In January 2017, the CBRC also issued a notice which requires banks to implement good data governance and customer information classification, protect the full life cycle of customer information, and perform regular information security risk assessments and internal audits.

Hong Kong SAR

Hong Kong has no single overarching cyber security law and the cyber regime is generally spread throughout different circulars and ordinances. Nonetheless, FIs operating in Hong Kong are subject to detailed technology risk management and data security requirements.

FS regulators emphasise the importance of building FI cyber resilience and strengthening cyber expertise. The chief executive of the HKMA has spoken of the importance of FIs and regulators working together to raise cyber security capabilities[26] and the SFC's Ashley Alder has identified cyber risk management as a major focus of firm inspections[27].

Recent FS regulatory developments:

HKMA Circular on Effective Cyber Security Risk Management

In September 2015, HKMA issued a circular to all authorised institutions (AIs) on the importance of effective cyber security risk management and giving guidance on this; for example having senior management play a proactive role[28].

HKMA Cyber Security Fortification Initiative

In May 2016 the HKMA launched its Cyber Security Fortification Initiative (CFI), which is made up of three components: the Cyber Resilience Assessment Framework (C-RAF), the Professional Development Programme (PDP) and the Cyber Intelligence Sharing Platform (CISP)[29].

The C-RAF is a self-assessment framework to help evaluate the inherent cyber security risks faced by FIs, determine whether their cyber resilience is commensurate with inherent risk and formulate ways to bridge gaps and enhance maturity. The first phase of the C-RAF will be carried out on FIs by September 2017 and there is also a plan to conduct simulation exercises based on current cyber intelligence by mid-2018[30]. The PDP aims to enhance cyber security expertise within FIs by providing local certification and training programs. The HKMA has more recently supplemented the PDP with the Enhanced Competency Framework on Cyber Security and Guidance[31]. The CISP has been described by the HKMA as a "one-stop shop for threat intelligence, alerts and solutions"[32] for industry, regulators and any other participants.

SFC Circulars

Hong Kong's other key FS regulator, the SFC, has cyber security as a supervisory priority[33] and has released several circulars on the issue in the past few years[34].

In March 2016, the SFC sent a circular to all licensed corporations about inadequacies identified during industry evaluations and urging all to ensure they review and assess risks, rectify any weaknesses and enhance controls. The circular included a list of cyber security controls seen by the SFC as sound and effective, such as: having a strong governance framework to supervise cyber security management; a formalised cyber security management process for service providers; pro-active identification and remediation of vulnerabilities and using information about the latest cyber-attack scenarios to enhance incident and crisis management procedures[35].

SFC Proposals to Reduce and Mitigate Hacking Risks

In May 2017, following a thematic review of the resilience to hacking risks of brokers engaged in internet trading, the SFC released proposed new requirements and measures to reduce and mitigate such risks[36]. These cover (i) preventative measures (e.g. two factor authentication, encryption of client login passwords and sensitive information) (ii) detective measures (e.g. monitoring and surveillance mechanisms, client notification) and (iii) other controls (e.g. a cyber risk management framework, training, crisis management).

India

Even though India is making leaps and bounds on the 'Digital India' initiative, it still does not have a cyber security framework. However, India's FS regulators have been active in the cyber security space.

The Information Technology Act (released in 2000 and amended in 2009) provides for certain aspects of cyber security and established the National Critical Information Infrastructure Protection Centre. The government also introduced the National Cyber Security Policy in 2013 to provide an umbrella framework for defining and guiding actions related to cyber security, with proposed strategies to include developing an assurance framework, strengthening regulation and promoting research and education. While the policy was well received, it has lacked an implementation framework and is yet to be adopted by industry.

Recent FS regulatory developments:
As early as 2011 the RBI released a comphrehensive set of guidelines on information security, electronic banking, technology risk management and cyber frauds[37], which covered securing the banking infrastructure spread across nine domains and multiple control objectives, and requiring enhancements to overall technology risk posture.

Reserve Bank of India measures

The RBI's active engagement has continued. In June 2016 the RBI issued a Circular on Cyber Security Frameworks in Banks that sets out detailed guidelines for such FIs. The RBI repeatedly encourages board and management level oversight and commitment on cyber security.

Requirements in the circular include: implementation of ISO/IEC 27001 and ISO/IEC 27002; a cyber security policy distinct from broader IT/IS policies; continuous surveillance; ensuring protection of customer information; having a cyber crisis management plan and reporting cyber security incidents and gap assessments to the RBI[38]. The RBI is also planning on conducting annual cyber audits[39] and has established a specialised cell (C-SITE) to conduct detailed IT examinations of banks' cyber security preparedness, to identify the gaps and to monitor the progress of remedial measures[40].

Insurance Regulatory and Development Authority measures

IRDAI meanwhile issued a cyber security framework for India's insurance sector in April 2017 that all insurers must implement by 31 March 2018[41]. Requirements are broadly in line with the RBI's approach: preparation of a gap analysis report, a board approved information and cyber security policy, a cyber crisis management plan and a chief information security officer responsible for articulating and enforcing policies to protect information assets.

Securities and Exchange Board of India measures

SEBI has also issued circulars laying down cyber security and cyber resilience frameworks that stock exchanges, clearing corporation and depositories[42], as well as national commodity derivatives exchanges[43], must comply with.

Requirements cover governance; identification and protection of critical IT assets; monitoring and detection of incidents, anomalies and attacks; response and recovery (e.g. through incident management, disaster recovery and business continuity frameworks); information sharing; training; and periodic audits.

SEBI is also planning on setting up a cyber security lab for the securities market during 2017 to 2018 and it has been reported that the regulator will appoint a chief information technology security officer to strengthen the cyber security regulatory policy framework[44].

Future trends

Looking into the horizon, additional standards or guidance on cyber security for FIs could be in the pipeline, given reports that India's Finance Minister is pushing for the set-up of a separate response team for cyber-attacks on the financial sector[45].

Figure 4: Views from the regulators

The dynamic nature of the cyber threat landscape means that a comprehensive and longterm commitment to cyber resilience must be embedded within organisations' culture.

Greg Medcraft
Chairman, Australian Securities and Investments Commission, 15 December 2016.

China is an internet power, and as one of the countries that faces the greatest internet security risks, urgently needs to establish and perfect network security legal systems.

Yang Heqing
National People's Congress Standing Committee.

Rather than harbouring the hope that you are lucky enough not to be targeted, it is more prudent and productive to take the necessary pre-emptive steps to protect yourself or your customers from cyber attacks.

Norman T.L. Chan
Chief Executive, Hong Kong Monetary Authority, 18 May 2016.

First and foremost, we expect the Board of Directors to get actively involved in the Technology related aspects. IT strategy needs to be closely aligned with the business strategy. With strides in technology, it would be difficult for Boards that do not have members having expertise in technology related areas to effectively adopt technology.

Mr S S Mundra
Deputy Governor of the Reserve Bank of India,
7 September 2016.

Moreover, the development of information technology has simultaneously refined the tactics of hackers and cyber-attacks. Particularly in the financial industries with global networks, once such an attack occurs in one location, its negative influence may spread across the board.

Haruhiko Kuroda
Governor of the Bank of Japan,
23 August 2016.

It is not inconceivable that the next financial crisis is triggered by a cyber attack. We need to develop the regulatory and supervisory capabilities to address these emerging threats. Cyber risk management will be the new frontier for global regulatory efforts and supervisory co-operation.

Mr Ravi Menon
Managing Director, Monetary Authority of Singapore,
20 March 2017.

Japan

Cyber security regulation in Japan is focused on being both secure and resilient and there has been a determined push to strengthen cyber risk management in the lead up to the 2020 Olympics.

Japan's 2014 Cybersecurity Basic Act includes provisions requiring infrastructure and cyber-related businesses to enhance cyber security and cooperate with the government, as well as measures around developing cyber talent, training and skills. Amendments to the Act have strengthened the authority of National Center of Incident Readiness and Strategy for Cyber Security (NISC), which analyses and responds to cyber attacks across government bodies. The 2015 Cyber Security Strategy sets out basic policy approaches and places emphasis on public-private cooperation, information sharing and promoting senior executive awareness[46]. Amendments to the Act on Promotion of Information Processing made in 2016 professionalise and raise standards of those who consult and give advice to businesses on cyber security.

Recent FS regulatory developments:

JFSA measures

The principal financial services regulator in Japan, the JFSA, has provided a set of guidelines around resilience building by FIs that includes developing internal regulations, leveraging the three lines of defence and helping establish a comprehensive cyber security framework that contributes to the greater ecosystem in the country. The regulator also conducted its first industry wide cyber security exercise (called Delta Wall) in October 2016 as part of its efforts to upgrade capability against cyber attacks[47].

FISC Guidelines

The Center for Financial Industry Information Systems (FISC) has also issued important guidelines and reports for the promotion of cyber risk management for FIs, most recently 2014's Report of the Council of Experts on Countermeasures Against Cyber-attacks on Financial Institutions[48].

Republic of Korea

Korean cyberspace is heavily regulated and the information technology regulatory regime is well established and comprehensive.

Korea was early to take regulatory action in regards to cyber security. For example, since 2004 it has required IT businesses to report hacks and in 2009 it set up the Korea Internet & Security Agency (KISA), a key government agency for identifying, preventing, and responding to cyber attacks and for ensuring strong cyber security. The nation's 2011 National Cyber Security Masterplan provides a framework for key initiatives. Other important developments have included the set-up of a Cyber Policy Department in 2013 and an announcement by the Ministry of Science, ICT, and Future Planning in 2014 of the creation of an index for private companies to evaluate their security levels[49].

Data localisation laws require storage and analysis of sensitive data within the country and FIs operating in the region are required to process data within Korea, unless the client provides written consent to do otherwise or if another exemption applies (e.g. as under EU and the U.S. trade agreements). The current focus is on refining and augmenting the existing framework to ensure it captures technological innovations. 2015's Act on the Development of Cloud Computing and Protection of Users is one example of authorities seeking to address risks associated with the growing use of cloud applications. Bolstering penalties for contraventions has also been done, as well as efforts to move from ex-ante to ex-post regulation in order to encourage organisations to adopt self initiated resilience building efforts.

Notable recent legislative and regulatory changes include:

- Act on the Development of Cloud Computing and Protection of Users (March 2015)
- Revisions to Regulation on Financial Institutions' Outsourcing of Data Processing Business & IT Facilities (Jun 2015)
- Revisions to Personal Information Protection Act and Promotion of IT Network Use and Information Protection Act (March 2016)
- Revisions to Regulation on Supervision of Electronic Financial Transactions (Oct 2016).

Recent FS regulatory developments:
Korea's key financial services regulator (the FSC) has long been interested in ensuring strong cyber security within FIs, particularly as many firms have been subject to major cyber attacks[50]. The importance of strong cyber security within FIs and for finance-related cyber networks was reiterated late last year by Korea's Finance Minister and Deputy Prime Minister (and former FSC chairman), whom also noted cyber security as having a key role in financial system stability[51].

FSC 2013 measures

In 2013, the regulator announced the Comprehensive Measures to Reinforce Financial Institution's Data Security, which set requirements such as establishing specialised data security teams, strengthening risk management capabilities, training experts and IT security guidelines[52].

FSC 2014 measures

Further measures were announced in 2014, such as requiring chief information security officer independence, CEO responsibility for contingency plans, monthly security inspections (with results reported to the CEO and the FSS), separation of intranet and internet networks, implementation of response systems and mandatory FSC registration of value added network providers[53].

Financial Security Institute

In 2015 the FSC approved the establishment of an independent financial security agency, the Financial Security Institute (FSI), which provides industry with comprehensive financial security services, including integrated financial security monitoring, computer emergency response and information sharing, vulnerabilities analysis and assessment, policy and technology research, education planning and management, information security certification and financial security conformance testing for new technologies and services[54].

Singapore

Singaporean authorities have had a longstanding interest in cyber risk and have launched a range of initiatives for creating a robust and resilient cyberspace.

In 2013, the Computer Misuse Act was amended to include cyber security measures and renamed the Computer Misuse and Cyber Security Act. In March 2016, the Cyber Security Agency of Singapore carried out Exercise Cyber Star, which saw 100 participants from banking and finance, government, energy and infocomm undertake scenario planning sessions and cyber attack simulations[55]. 2016 also saw the launch of the TechSkills Accelerator initiative to help the workforce acquire new ICT skills such as cyber security[56] and the release of Singapore's Cyber Security Strategy.[57] It is the latest policy document to outline medium and long-term strategies aiming to strengthen the resilience of critical information infrastructure, creating a safer cyberspace, developing a vibrant cyber security ecosystem with skilled professionals and forging strong international partnerships. This year, legislation may be introduced that will include mandatory breach reporting and powers to conduct cyber audits of businesses[58].

Recent FS regulatory developments: Singapore's FS regulator, MAS, has taken an active interest in enhancing cyber security amongst the regulated population. MAS' Bernard Wee has commented that "a successful cyber-attack is no longer a question of 'if' but a question of 'when' " and has spoken about the need for FIs to adopt a multi-pronged approach to enhancing their cyber resilience capabilities and to ensure they have resources that will enable a safe and swift recovery of systems and operations[59]. In addition to guidelines on resilience building, MAS has placed a great emphasis on AML/CTF and outsourcing risk.

MAS Circular No. SRD TR 03/2015 Technology Risk and Cyber Security Training for Boards

In late 2015, MAS issued a circular detailing the regulator's expectations that boards will take responsibility for technology risks and cyber security; ensure appropriate accountability structure and organisational risk culture to support effective implementation of cyber resilience programs; have comprehensive technology risk and cyber security training and be regularly apprised on salient technology and cyber risk developments[60].

MAS Circular No. SRD TR 01/2015 Early Detection of Cyber Intrusions

Also in 2015, MAS provided guidance on the early detection of cyber intrusions, noting that "strong cyber resilience requires robust capabilities to promptly detect any cyber intrusions so as to enable swift containment and recovery". Some of the key elements identified were: having control processes to monitor and detect internal and external intrusions; thorough investigations to determine extent of infiltration and damage; immediate actions to contain impact; a tested cyber breach response plan; regular gap analysis and risk assessments; and the continual evolution and improvements of processes to anticipate, withstand, detect, and respond to cyber-attacks[61].

Asia Pacific Regional Intelligence and Analysis Centre

In December 2016, MAS announced a collaboration to establish the Asia Pacific Regional Intelligence and Analysis Centre, which will monitor cyber threats to member FIs in the region, provide analysis and recommend courses of action to mitigate threats[62].

Recommendations

Cyber attacks can be extremely damaging for FIs, and unfortunately they are here to stay. As such, a focus on robust management of cyber risk remains critical. The active development of cyber security regulation across APAC jurisdictions will also continue to progress and FIs will need to ensure that they keep pace with changes and refinements. While it may seem that there are many emerging regulations and standards, the underlying direction and overarching themes are clear. Cyber programs that are designed with security, vigilance and resilience in mind, guided by a clear strategy and supported by strong governance measures, will be well placed to meet evolving standards.

01

Set a risk appetite

Understand the business and strategic context to set cyber risk appetite and desired target state. Incorporate the cyber risk appetite into existing risk management and governance processes.

02

Develop a cyber strategy

Develop an executive led cyber strategy based on unique business needs and threats. Make sure this is not isolated within the IT department, for example by incorporating cyber security strategy into the enterprise risk management framework.

03

Keep the board and executive involved

Ensure that the board and executives are made aware of and are actively involved in cyber risk management, through regular meetings and updates on cyber risks, mitigation activities and potential business impacts.

04

Build a cyber risk culture

Embed cyber risk values and behaviors into firm culture by building a cyber risk aware workforce. Strong leadership, a coordinated communications plan, training and continuous learning, and appropriate skills recruitment are all important elements.

05

Regular vulnerability assessments and penetration testing

Conduct regular vulnerability assessments and penetration testing to ensure defence preparedness and early detection of security loopholes. As attacks change, update policies, procedures and drills to cover new threats.

06

Establish a dynamic contingency plan

An incident contingency plan should include documenting attack details, data backup, measures to prevent damage spreading and for mitigating disruptions to critical business processes, as well as root cause analysis. Continually test, review and improve, including through executive war gaming.

07

Stay informed

Keep informed of the latest and emerging cyber threats, security developments, industry standards and regulatory thinking. Incorporate learnings into internal discussions, policies, procedures and processes.

08

Review and iterate

Adopt a proactive and adaptive approach by regularly reviewing and iterating governance and cyber response strategies to ensure their continuing effectiveness and alignment with business strategy and regulatory expectations.

09

Enlist innovative solutions

Consider investing in innovative digital solutions, which can facilitate the implementation of security procedures across a large organisation and reduce the speed at which attacks evolve.

10

Engage externally

Engage with peers and regulators to encourage information sharing, cooperative and coordinated responses and the development of harmonised standards.

References

1. Deloitte **Building trust across cultures: Privacy and data protection** (March 2017) https://www2.deloitte.com/vi/en/pages/risk/articles/gx-building-trust-across-cultures.html
2. Commonwealth of Australia **Australia's cyber security strategy: Enabling innovation, growth & prosperity** (April 2016) https://cybersecuritystrategy.dpmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf
3. Symantec **Internet Security Threat Report Volume 21** (April 2016) https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf
4. Ashley Alder, CEO Hong Kong Securities and Futures Commission **Keynote Remarks at the Hedge Fund Standards Board Institutional Investor Roundtable** (22 June 2016) http://www.sfc.hk/web/EN/files/ER/PDF/Speeches/Ashley_20160622.pdf
5. IOSCO **FR02/2016 Cyber Security in Securities Markets - An International Perspective, Report of the Board of IOSCO** (6 Apr 2016) https://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf
6. IOSCO **Securities Markets Risk Outlook 2016, Report of the IOSCO Research Function** (2 Mar 2016) https://www.iosco.org/library/pubdocs/pdf/IOSCOPD527.pdf
7. SWIFT **SWIFT introduces mandatory customer security requirements and an associated assurance** (27 September 2016) https://www.swift.com/insights/press-releases/swift-introduces-mandatory-customer-security-requirements-and-an-associated-assurance-framework
8. Deloitte **Beneath the surface of a cyberattack: A deeper look at business impacts** (2016) http://www2.deloitte.com/us/en/pages/risk/articles/hidden-business-impact-of-cyberattack.html
9. Commonwealth of Australia **Australia's cyber security strategy: Enabling innovation, growth & prosperity** (April 2016) https://cybersecuritystrategy.dpmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf
10. Symantec **Internet Security Threat Report Volume 21** (April 2016) https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf
11. Arun Devnath and Michael Riley **Bangladesh Bank Heist Probe Said to Find Three Hacker Groups** Bloomberg https://www.bloomberg.com/news/articles/2016-05-10/bangladesh-bank-heist-probe-said-to-find-three-groups-of-hackers
12. Saloni Shukla & Pratik Bhakta **3.2 million debit cards compromised** Economic Times (20 October 2016) http://economictimes.indiatimes.com/industry/banking/finance/banking/3-2-million-debit-cards-compromised-sbi-hdfc-bank-icici-yes-bank-and-axis-worst-hit/articleshow/54945561.cms
13. **After US$65m hack, questions of whether Bitcoin can be safe** The Business Times (18 August 2016) http://www.businesstimes.com.sg/banking-finance/after-us65m-hack-questions-of-whether-bitcoin-can-be-safe
14. John Liu **Russian suspects flee Taiwan after stealing US$2.17m from ATMs Asia News Network** (12 July 2016) http://www.asianews.network/content/russian-suspects-flee-taiwan-after-stealing-us217m-atms-22484
15. **South Korea in 'emergency mode' over cyber threat to banks** Financial Times (22 June 2017) https://www.ft.com/content/cb2db9f8-5700-11e7-9fed-c19e2700005f?mhq5j=e1
16. Deloitte **Asia-Pacific Defense Outlook 2016: Defense in Four Domains** (2016) https://www2.deloitte.com/global/en/pages/public-sector/articles/gx-asia-pacific-defense-outlook.html
17. Commonwealth of Australia **Australia's cyber security strategy: Enabling innovation, growth & prosperity** (April 2016) https://cybersecuritystrategy.dpmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf
18. Australian Government, Department of Prime Minister and Cabinet The Hon Dan Tehan MP, Minister Assisting the Prime Minister for Cyber Security (20 July 2016) https://www.dpmc.gov.au/news-centre/cyber-security/hon-dan-tehan-mp-minister-assisting-prime-minister-cyber-security
19. For example, while not specifically mentioning cyber security, s912A of the Corporations Act 2001 (administered by ASIC) requires all Australian financial services licensees to have adequate technological resources and risk management systems. APRA standards also do not specifically mention cyber security but CPS 220 Risk Management requires proper risk management strategies, including IT systems, while CPG 234 Management of Security Risk in Information and IT and CPG 235 Managing Data Risk provide guidance about data and security risks.
20. ASIC **ASIC'S Corporate Plan 2016–17 to 2019–20** (August 2016) http://download.asic.gov.au/media/3997927/corporate-plan-2016-published-31-august-2016.pdf
21. ASIC **Embedding cyber resilience within company culture** (April 2016) http://asic.gov.au/regulatory-resources/markets/resources-on-markets/markets-articles-by-asic/embedding-cyber-resilience-within-company-culture/
22. APRA **Information Paper: 2015/16 Cyber Security Survey Results** (September 2016) http://www.apra.gov.au/AboutAPRA/Documents/Information-Paper-Cyber-Security-2016-v4.pdf
23. ASIC **Report 429 Cyber resilience: Health check** (March 2015) http://download.asic.gov.au/media/3062900/rep429-published-19-march-2015-1.pdf
24. ASX **ASX 100 Cyber Health Check Report: Capturing the opportunities while managing the threats** (April 2017) http://www.asx.com.au/documents/investor-relations/ASX-100-Cyber-Health-Check-Report.pdf
25. **Privacy Amendment (Notifiable Data Breaches) Bill 2016**, http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r5747
26. Norman T.L. Chan, CEO HKMA K**eynote Address at Cyber Security Summit 2016** (18 May 2016) http://www.hkma.gov.hk/eng/key-information/speech-speakers/ntlchan/20160518-2.shtml
27. Ashley Alder CEO **SFC Keynote remarks at Hedge Fund Standards Board Institutional Investor Roundtable** (22 June 2016) http://www.sfc.hk/web/EN/files/ER/PDF/Speeches/Ashley_20160622.pdf
28. HKMA **Circular: Cyber Risk Management** (15 September 2015) http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2015/20150915e1.pdf
29. HKMA **Launch of the Cybersecurity Fortification Initiative by the HKMA at Cyber Security Summit 2016** (18 May 2016) http://www.hkma.gov.hk/eng/key-information/press-releases/2016/20160518-5.shtml
30. HKMA **Circular: Cybersecurity Fortification Intiative** (21 December 2016) http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2016/20161221e1.pdf
31. HKMA **Circular: Enhanced Competency Framework on Cybersecurity** (19 December 2016) http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2016/20161219e1.pdf

32. Howard Lee, Senior Executive Director HKMA **Cyber resilience through collaboration: Visions and actions of the HKMA** (21 September 2016) http://www.hkma.gov.hk/media/eng/doc/key-information/speeches/s20160921e1.pdf
33. SFC **Regulation for Quality Markets: Annual Report 2016-2017** (June 2017) http://www.sfc.hk/web/EN/files/ER/Annual%20Report/SFC_Annual_Report_2016-17_Eng.pdf
34. For example Circular on Tips on Protection of Online Trading Accounts (29 January 2016), Circular on Internet Trading – Internet Trading Self-Assessment Checklist (11 June 2015), Circular on Mitigating Cyber security Risks (27 November 2014), Circular on Internet Trading – Information Security Management and System Adequacy (26 November 2014), and Circular on Internet Trading – Reducing Internet Hacking Risks (27 January 2014).
35. SFC **Circular to All Licensed Corporations on Cybersecurity** (23 March 2016) http://www.sfc.hk/edistributionWeb/gateway/EN/circular/doc?refNo=16EC17
36. SFC **Consultation Paper on Proposals to Reduce and Mitigate Hacking Risks Associated with Internet Trading** (May 2017) http://www.sfc.hk/edistributionWeb/gateway/EN/consultation/openFile?refNo=17CP4
37. RBI **Guidelines on Information security, Electronic Banking, Technology risk management and cyber frauds** (2011) https://rbidocs.rbi.org.in/rdocs/content/PDFs/GBS300411F.pdf
38. RBI **Cyber Security Framework in Banks** (2 June 2016) https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=10435&Mode=0
39. India Briefing **Central Bank Directive to Tighten Cyber Security after Debit Card Data Breach** (24 October 2016) http://www.india-briefing.com/news/india-regulatory-brief-banks-cyber-security-compliance-fssai-steps-up-inspections-12973.html/
40. S S Mundra, **RBI Deputy Governor Keynote Address at the Seminar on Financial Crimes Management** (30 January 2017) http://www.bis.org/review/r170202d.htm
41. IRDAI **Circular IRDA/IT/GDL/MISC/082/04/2017 Guidelines on Information and Cyber Security for insurers** (7 April 2017) https://www.irdai.gov.in/ADMINCMS/cms/frmGuidelines_Layout.aspx?page=PageNo3118
42. SEBI **Circular CIR/MRD/DP/13/2015 Cyber Security and Cyber Resilience framework of Stock Exchanges, Clearing Corporation and Depositories** (6 July 2015) http://www.sebi.gov.in/cms/sebi_data/commondocs/1436179654531_p.pdf
43. SEBI **Circular SEBI/HO/CDMRD/DEICE/CIR/P/2016/0000000044 Cyber Security and Cyber Resilience framework of National Commodity Derivatives Exchange**s (29 March 2016) http://www.sebi.gov.in/cms/sebi_data/attachdocs/1459250540053.pdf
44. Times of India **Sebi to beef up cyber security framework for markets** (25 September 2016) http://timesofindia.indiatimes.com/business/india-business/Sebi-to-beef-up-cyber-security-framework-for-markets/articleshow/54507980.cms
45. Pratik Bhakta, **Economic Times FM pushes for setting up of separate Response Team for Cyber-attacks on the financial sector** (1 February 2017) http://economictimes.indiatimes.com/industry/tech/internet/fm-pushes-for-setting-up-of-separate-response-team-for-cyber-attacks-on-the-financial-sector/articleshow/56909353.cms
46. Government of Japan **Cybersecurity Strategy** (4 September 2015) https://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf
47. JFSA **First industry-wide cyber security exercise ("Delta Wall")** (20 October 2016) http://www.fsa.go.jp/en/newsletter/weekly2016/216.html
48. FISC **Report of the Council of Experts on Countermeasures Against Cyber-attacks on Financial Institutions** (26 February 2014) https://www.fisc.or.jp/data/english/pdf/FISC_Report_February26_2014.pdf
49. ZDNet **Korea introduces security readiness guideline for private sector** (15 August 2014) http://www.zdnet.com/article/korea-introduces-security-readiness-guideline-for-private-sector/
50. Notable are the 2009 and 2011 denial-of-service attacks on several Korean banks online services and the 2014 leak of more than 100 million customers' data from three credit card firms.
51. Yonhap News Agency **Financial authorities on high alert against cyberthreats** (12 December 2016) http://english.yonhapnews.co.kr/northkorea/2016/12/12/43/0401000000AEN20161212011100320F.html
52. FSC **Comprehensive Measures to Reinforce Financial Institution's Data Security** (17 July 2013) https://financialservicescommission.wordpress.com/2013/07/17/comprehensive-measures-to-reinforce-financial-institutions-data-security/
53. FSC Comprehensive Measures to Protect Personal Data in the Financial Sector (10 March 2014) https://www.fsc.go.kr/downManager?bbsid=BBS0048&no=89679
54. Financial Security Institute http://www.fsec.or.kr/fseceng/index.do
55. Singapore Ministry of Information and Communications **CSA marks operational milestone with Exercise Cyber Star** (22 March 2016) https://www.csa.gov.sg/news/press-releases/exercise-cyber-star
56. InfoComm Media Development Authority **New TechSkills Accelerator to Help Develop Core and Sector-Specific ICT Skills** (May 2016) https://www.imda.gov.sg/about/newsroom/archived/ida/media-releases/2016/new-tech-skills-accelerator-to-help-develop-core-and-sector-specific-ict-skills
57. Singapore Ministry of Information and Communications **Singapore's Cybersecurity Strategy** (October 2016) https://www.csa.gov.sg/~/media/csa/documents/publications/singapore-cybersecuritystrategy.pdf?la=en
58. Channel Asia **News New Cybersecurity Act to be tabled in 2017: Yaacob Ibrahim** (11 April 2016) http://www.channelnewsasia.com/news/singapore/new-cyber security-act-to/2685052.html
59. Bernard Wee, MAS Executive Director **A Bold Approach to Cyber Risk Management** (16 May 2016) http://www.mas.gov.sg/News-and-Publications/Speeches-and-Monetary-Policy-Statements/Speeches/2016/A-Bold-Approach-to-Cyber-Risk-Management.aspx
60. MAS **Circular No. SRD TR 03/2015 Technology Risk and Cyber Security Training for Board** (9 October 2015) http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/TRS%20Circulars/Circular%20TR03%202015%20%20Technology%20Risk%20and%20Cyber%20Security%20Training%20For%20Boa.pdf
61. MAS **Circular No. SRD TR 01/2015 Early Detection of Cyber Intrusions** (24 August 2015) http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/TRS%20Circulars/SRD%20TR%200115%20%20Early%20detection%20of%20cyber%20intrusions.pdf
62. MAS **FS-ISAC and MAS Establish Asia Pacific (APAC) Intelligence Centre for sharing and analysing cyber threat information** (1 December 2016) http://www.mas.gov.sg/News-and-Publications/Media-Releases/2016/FS-ISAC-and-MAS-Establish-APAC-Intelligence-Centre.aspx

Contacts

Australia

Kevin Nixon
Partner, Risk Advisory
+61 2 9322 7555
kevinnixon@deloitte.com.au

James Nunn-Price
Partner, Risk Advisory
+61 2 9322 7971
jamesnunnprice@deloitte.com.au

Puneet Kukreja
Partner, Risk Advisory
+ 61 3 9671 8328
pkukreja@deloitte.com.au

China & Hong Kong

Tony Wood
Partner, Risk Advisory
+852 2852 6603
tonywood@deloitte.com.hk

Eva Kwok
Partner, Risk Advisory
+852 28526304
evakwok@deloitte.com.hk

Boris Zhen Zhang
Director, Risk Advisory
+86 21 61411505
zhzhang@deloitte.com.cn

India

Shree Parthasarathy
Partner, Risk Advisory
+91 124 679 2355
sparthasarathy@deloitte.com

Gautam Kapoor
Partner, Risk Advisory
+91 124 679 2409
gkapoor@DELOITTE.com

Japan

Tsuyoshi Oyama
Partner, Risk Advisory
+81 90 9834 4302
tsuyoshi.oyama@tohmatsu.co.jp

Hiroshi Sakui
Partner, Risk Advisory
+81 70 6473 7675
hiroshi.sakui@tohmatsu.co.jp

Mitsuhiko Maruyama
Partner, Risk Advisory
+81 90 6492 3648
mitsuhiko.maruyama@tohmatsu.co.jp

Korea

Young Soo Seo
Partner, Risk Advisory
+82 2 6676 1929
youngseo@deloitte.com

Singapore

Thio Tse Gan
Partner, Risk Advisory
+65 6216 3658
tgthio@deloitte.com

Deloitte.

MCBD_HYD_06/17_054593