Asian Regulatory Round Up
IMAS Conference
February 2016

Themes for Asset Management

- Size, substance and fiduciary duties
- Culture of compliance and senior management responsibility
- Tax / KYC / AML
- Investor protection vs caveat emptor and nationalism
- Manipulation / rigging / collusion
- OTC reporting / trading /clearing and cost of doing business
- Risks of outsourcing and cybersecurity threats

Too Big to Fail

- 2015 deadline for declaring FMCs to be global SIFIs passed
  - Non decision not an active conclusion
  - Persuaded by segregation of assets and fiduciary duties
  - Concerns about flight of capital from banking to asset management
- Perceived regulatory risks means more FMC regulation to come
  - Managers not actually exercising fiduciary duties
  - Abrupt withdrawal of an important manager could cause dry up in liquidity
  - Fire sales where managers sell into a crashing market due to large withdrawals, investment restrictions and or risk or margin considerations
  - Asset managers relying on complicated derivatives positions or high levels of leverage to achieve returns represent counterparty and model risk
  - Funds with daily or short-term redemptions but invest in illiquid or long-term assets

Substance and Presence

- National regulators concerns about viability of FMCs
  - Permanent presence required to access local markets
  - Experience of staff as bankers move into asset management
  - Viability of business plans in crowded market
  - Sufficiency of investment in operational support and technology
  - Appropriateness of internal controls and risk management
  - Issues with tax driven FMC structures
- Conflicts of interest concerns
  - Too many business interests
  - Cross directorships
  - Co-investment

Culture of Compliance

I reject the narrative that the current state of affairs is simply the result of the actions of isolated rogue traders or a few bad actors within these firms. As James O'Toole and Warren Bennis observed in their Harvard Business Review article about corporate culture: "Ethical problems in organizations originate not with 'a few bad apples' but with the 'barrel makers'. That is, the problems originate from the culture of the firms, and this culture is largely shaped by the firms' leadership. This means that the solution needs to originate from within the firms, from their leaders

What do I mean by the culture within a firm? Culture relates to the implicit norms that guide behavior in the absence of regulations or compliance rules—and sometimes despite those explicit restraints. Culture exists within every firm whether it is recognized or ignored, whether it is nurtured or neglected, and whether it is embraced or disavowed. Culture reflects the prevailing attitudes and behaviors within a firm. It is how people react not only to black and white, but to all of the shades of grey. Like a gentle breeze, culture may be hard to see, but you can feel it. Culture relates to what "should" I do, and not to what "can" I do.

William Dudley President Fed Reserve Bank

Senior Management Responsibility

- Tone at the Top
  - Example that senior leaders set is critical to an institution's culture
  - Senior leaders need to hold up a mirror to their own behavior and critically examine behavioral norms at their firm.
  - Senior leaders must take responsibility for the solution and communicate frequently, credibly and consistently about the importance of culture.
  - Boards of directors have a critical role to play in setting the tone and holding senior leaders accountable for delivering sustainable change

How to Build Culture

- Comprehensive approach to improving their culture that encompasses recruitment, onboarding, career development, performance reviews, pay and promotion
  - Employee surveys and 360 feedback processes to target issues of behavior and culture.
  - Case study discussions into training programs to highlight ethical dilemmas and decision-making.
  - Revamping senior level promotion criteria to reinforce what are the desired characteristics and behaviors of leaders
  - Anonymous culture survey would be fielded across firms each year by an independent third-party
  - Open routine escalation of issues, consistent application of “should we” vs “could we” in decisions, rigor in identifying and controlling of conduct risk, and compliance breaches factoring into compensation.
- Promote effective self-policing
  - If audit uncovers fraud in one unit firm should ask, “Where else could this behavior occur?”
  - If fraud at competitor ask “Could this happen to us, could we have a similar problem here?”
  - When fraud is detected, boards and senior leaders must ensure that they are informed promptly, and that a thorough inquiry is undertaken at once.
  - Early self-reporting sends powerful message to employees and t regulators about a respect for law
- Individuals should feel they can raise a concern, and have confidence that the issues will be escalated and considered

Mutual Recognition of Funds – Hong Kong and China*	
China funds heading south	Hong Kong funds heading north
Initial quota: RMB300 billion (USD46 billion).	Initial quota: RMB300 billion (USD46 billion).
Registered, established and managed in Mainland in accordance with PRC Laws.	Established and Domiciled in Hong Kong, authorised by the HK SFC.
Publically offered fund registered with CSRC.	Publically offered fund authorised by the SFC.
More than 12 months old.	More than 12 months old.
Minimum size RMB200 million (USD32 million).	Minimum size USD32 million (RMB200 million).
Must not invest more than 20% in Hong Kong.	Must not invest more than 20% in China.
Not more than 50% of assets under management may be sold to Hong Kong investors.	Not more than 50% of AUM may be sold to China investors.
Only general equity funds, bond funds, mixed funds, index funds and physical ETFs allowed.	Only general equity funds, bond funds, mixed funds, index funds and physical ETFs allowed.
Existing offering documents may be used, supplemented with bilingual (English/Chinese) Hong Kong-covering document. KFS required.	Existing offering documents may be used, supplemented with Chinese-covering document.
Must appoint Hong Kong representative with (min) Type 1 Licence.	Must appoint Mainland agent, qualified to offer funds in China.
Up to 850 funds currently eligible.	Around 100+ unit trusts currently eligible.

Asia Region Fund Passport

APEC – Asia Region Funds Passport*
Announcement by APEC Finance Ministers on 22 September 2013. New Statement of Understanding (SoU) issued on 11 September 2015.
Originally involved Australia, South Korea, Singapore and New Zealand. SoU confirmed participation of Australia, Japan, New Zealand, South Korea, The Philippines, and Thailand, but the exclusion of Singapore.
Expected implementation in 2016.
Based on an ASIC initiative from 2008.
APEC has issued draft and Operational Arrangements, seeking feedback from the market. Joint Public Consultation in 2014 (on Rules and Arrangements) completed. Consultation Paper issued April 2014.
Extensive responses from industry delivered in April 2015.
Scheme more focused on export of funds from Australia and Korea than on import.
Fundamental problems on fund importation in Australia and Korea due to unfavourable taxation. Need to have neutral tax acknowledged.
Each market allowed to decide whether to participate (or not).
Only when two or more participants have agreed Rules, can scheme be launched.
Launch scheduled for H1 2016.
Primary objective: to become the Asia-Pacific UCITS equivalent.

Product Nationalism

- Asian AUM in UCITS is USD200 billion – 5% of total AUM
  - 4500 UCITS registered in Singapore, HK and Taiwan
- Asian government keen to keep this money in the region
  - Clear no room for UCITS in 3 Asian fund passports
  - Only feeder funds would be option
- Challenges to this
  - No real local alternative for US, European, Japanese, global or fixed income mandates
  - Current structure with global investment expertise sitting outside Asia would need to change
  - Estimate that HK domiciled funds 100 bps lower TERs
- Opportunities for UCITS
  - Providers used to domiciling funds in one location and managing / / marketing them in others

Tax / KYC / AML

- OECD CRS
  - Automatic exchange of information with systematic and annual transmission of “bulk” taxpayer information by source jurisdiction to residence jurisdiction of taxpayers
  - Aim - to provide timely information on non-compliance where tax has been evaded
  - 90 jurisdictions expected to adopt CRS and 61 signed up at June 2015
  - 50 “early adopter” jurisdictions with first reporting from September 2017
  - Early adopter countries need new account opening procedures to be in place from 1 January 2017
  - Singapore not yet signed the CRS but impact felt as fund domiciles have signed

CRS Resources

CA | ComplianceAsia

CRS Resources - Forms

WHAT'S NEW

February 2016

› **Self-certification forms** : *The **Business and Industry Advisory Committee to the OECD** (BIAC) has drafted the following self-certification forms and has requested the OECD to make these forms available on the AEOI Portal to assist with the implementation of the CRS. The OECD has not approved the forms and neither the OECD nor BIAC regard them as mandatory or as best practice documents. They serve only to illustrate how financial institutions may consider requesting customer information from their accountholders. Financial institutions should consult their advisers to ensure their CRS-related operations, including the self-certification forms collected from accountholders, comply with all applicable national laws. BIAC is an independent international business association devoted to giving the OECD business perspectives on a broad range of global policy issues.*

> Controlling Person tax residency self-certification form

> Entity tax residency self-certification form

> Individual tax residency self-certification form

CRS Resources - Countries

CRS by jurisdiction

This section will provide you with a jurisdiction-specific overview of the steps taken and choices made by jurisdictions in the context of implementing the Standard. The overview table below will show the current state of implementation of all committed jurisdictions in a single table. In case you would like to have more detailed information about the current state of implementation of the Standard in a particular jurisdiction, you will be able to access jurisdiction-specific legislation by clicking on the green tick relating to that jurisdiction.

2017/2018

Updated on 10 February 2016

A B C D E F G H I J K L M N P Q R S T U

Jurisdiction	Committed to first exchange in	Primary legislation	Secondary legislation	Guidance	List of low risk non-reporting FIs and excluded accounts	Domestic Reporting Format
Anguilla	2017					
Argentina	2017	✓	✓	✓	✓	✓
Barbados	2017	✓				
Belgium	2017	✓	✓		✓	✓
Bermuda	2017	✓	n.a.			
British Virgin Islands	2017	✓			✓	

CA | ComplianceAsia

2013 - G8 Action Plan

- **Companies should know who owns and controls them and their beneficial ownership** and basic information should be adequate, accurate, and current. Companies should be required to obtain and hold their beneficial ownership and basic information, and ensure documentation of this information is accurate.
- **Beneficial ownership information on companies should be accessible onsho**re to law enforcement, tax administrations and other relevant authorities including, financialintelligence units. This could be achieved through central registries of company beneficialownership and basic information at national or state level. Countries should consider measures tofacilitate access to company beneficial ownership information by financial institutions and other regulated businesses. Some basic company information should be publicly accessible.
- **Trustees of express trusts should know the beneficial ownership of the trust**, including informationon beneficiaries and settlors. This information should be accessible by law enforcement, tax administrations and other relevant authorities including financial intelligence units.

2013 - G8 Action Plan

- **Authorities should understand the risks to which their anti-money laundering and countering the financing of terrorism regime is exposed and implement effective and proportionate measures to target those risks.** Appropriate information on the results of the risk assessments shouldbe shared with relevant authorities, regulated businesses and other jurisdictions.
- **The misuse of financial instruments and of certain shareholding structures** which may obstruct transparency, such as bearer shares and nominee shareholders and directors, should be prevented.
- **Financial institutions and designated non financial businesses and professions, including trust and company service providers, should be subject** to effective anti money laundering andcounter terrorist financing obligations to identify and verify the beneficial ownership of theircustomers. Countries should ensure effective supervision of these obligations.
- **Effective, proportionate and dissuasive sanc**tions should be available for companies, financialinstitutions and other regulated businesses that do not comply with their respective obligations,including those regarding customer due diligence. These sanctions should be robustly enforced.
- **National authorities should cooperate effectively domestically and across borders** to combat theabuse of companies and legal arrangements for illicit activity. Countries should ensure that their relevant authorities can rapidly, constructively, and effectively provide basic company and beneficial ownership information upon request from foreign counterparts.

Latest AML / CDD Developments

- June 2015 - EU published AMLD IV
  - More alignment with US standards but also new requirements
  - More risk based approach requiring evidence based assessment of risks associated with AML
  - Fewer due diligence exemptions – regulated institutions not automatically eligible for SDD must be specific customer profile
  - PEP now includes domestic politicians and SOEs
  - EU member states required to create registries of beneficial owners of companies
  - Lower reportable cash payment threshold to E7,500
  - Minimum requirements so EU states can impose higher requirements
  - 2 year implementation period

Latest AML / CDD Developments

- August 2015 - FinCen published AML standards
  - Requires SEC registered investment advisers to have AML programmes
- AML programme requires adviser to:-
  - Establish and implement policies, procedures and internal controls reasonably designed to ensure compliance and prevent ML / TF
  - Have periodic independent testing to assess compliance with rules. May be third party or its affiliates' or employees but employees must not involved in the operation AML program. Frequency depends on ML / TF risk assessment
  - Designate an individual or a committee responsible for the AML program
  - Train employees and relevant agents and third-party service providers
  - Require advisers to file STRs with FinCen over US$5000

Latest AML / CDD Developments

- FinCen risk factors for individuals, pooled entities, non pooled entities
  - Ownership status of investor (publicly traded vs private)
  - Identities of ultimate owners / beneficiaries of private entities
  - Geographic location of investor
  - Source of funds for investor subscriptions and location to which investor funds are distributed
  - PEP status of investor
  - Existing regulatory oversight of investor
  - Unusual or inconsistent information provided at time of subscription
  - Experience adviser has with the investor
  - References from other financial institutions

Latest AML / CDD Developments

- Investor deemed suspicious at time of subscription if he
  - Has unusual concern about adviser's compliance with government reporting
  - Reluctant or refuses to give information about business activities
  - Provides unusual identification or business documents
  - Appears to be acting as agent but refuses to provide information
  - Shows lack of concern about investment returns or risks
- Suspicious activities at time of subscription or withdrawal
  - Subscription by new investor with early or frequent withdrawal
  - Unexplained changes in wiring instructions
  - Pattern of withdrawals contrary to stated investment objectives
  - Funding a managed account or subscribing via multiple wire transfers from different accounts at different financial institutions
  - Structural or geographic changes that increase risk – HQ moves to high risk country

Latest AML / CDD Developments

- Outsource AML programme to transfer agent or administrator must perform due diligence on its
  - Latest AML policies and procedures
  - Results of regulatory examinations or latest annual audit
  - Expertise in performing AML controls
  - Operational resilience especially regarding cyber incidents
  - Legal and regulatory compliance / IT and physical security / incident reports
- Contracts to have up to date risk controls and legal protection for adviser and clearly define agent's and adviser's responsibility for compliance with each specific law
- Monitor agent's performance
  - Periodic onsite visits to agent
  - Ongoing review of agents reliance and exposure to sub-contractors
  - Identifying conflicting interests
  - Verify ability to timely remediate adviser complaints

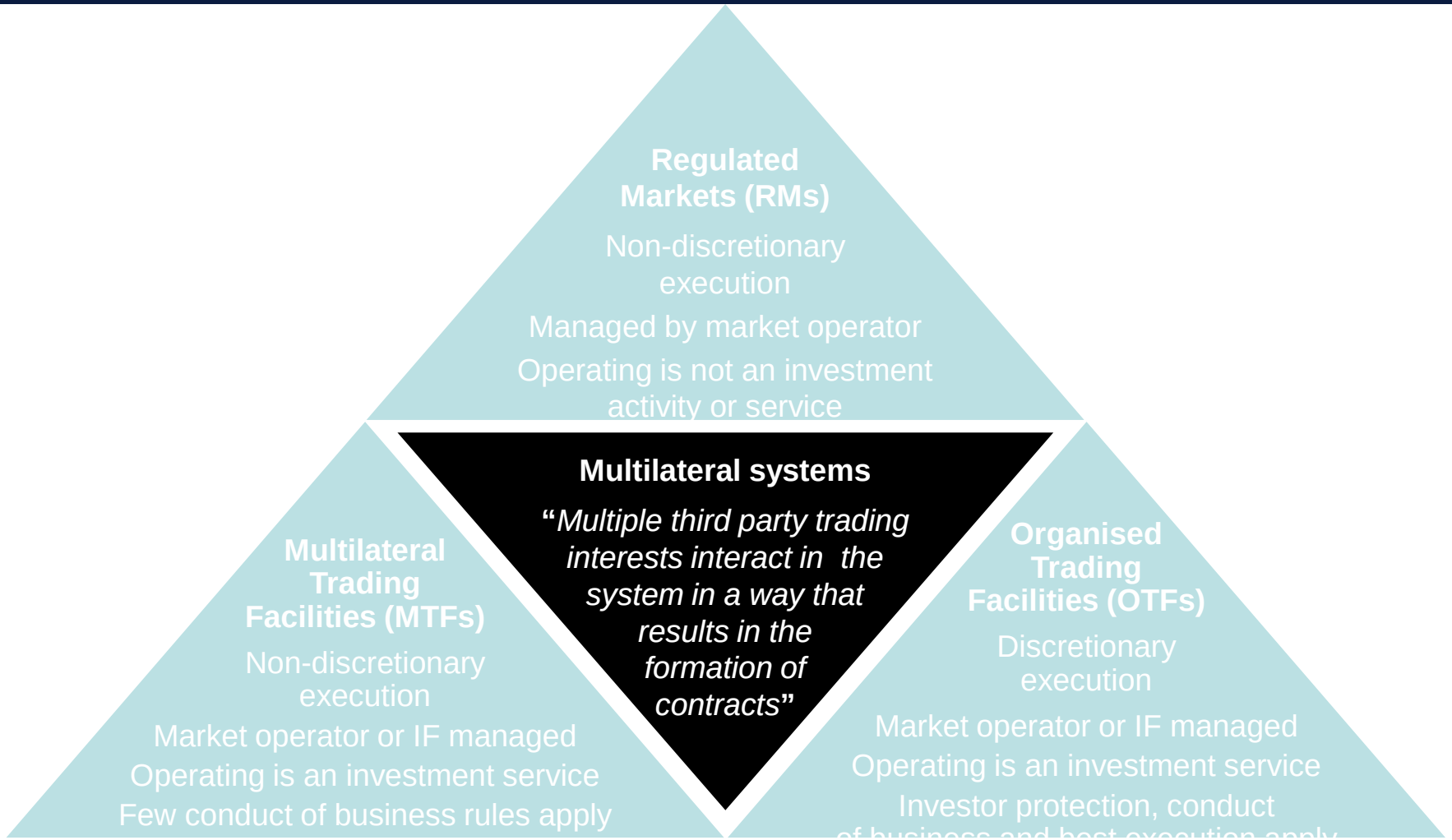
OTC - Why all the changes?

- Following GFC G20 aim to reduce systemic risk and risk of disruption in derivatives market
- Broad aim – bring dark private transactions into lit trading arena
- Required enactment into national laws
  - In EU via EMIR and MiFID II
  - In US via Dodd Frank and set up of CFTC
  - In Asia each country requires own laws
- Significant challenges to timelines and implementation

Stage 1 - Derivative Reporting

- Data relating to derivatives and counterparties submitted to a trade repository
- Trade repository is regulated organisation established to manage data
  - Promote transparency by making information on derivatives provided to trade repositories available to regulators
  - Accurate overview of derivatives market and exposures of market participants to aid prudential regulation of financial markets
- LEI is Legal Entity Identifier
  - Development of a global unique identification system for parties to financial transactions
  - January 2013 LEI Regulatory Oversight Committee has responsibility for development and implementation of global LEI system.

Stage 2 - Trading



Stage 3 - OTC Clearing

- Clearing for OTC derivatives
  - Process by which two parties to OTC derivative contract replace it with two separate contracts with central counterparty
  - CCP takes over each party's positions under original contract
  - Two parties no longer have contract with each other but instead with CCP making CCP counterparty to each of original parties
- Aim to promote financial stability by reducing counterparty credit risk and operational burdens
  - Parties become exposed to CCP's credit risk not each other
  - Increasing transparency
  - Standardising default management process

Clearing Models

- Member Clearing
  - Market participant becomes clearing member of CCP
  - Onerous requirements imposed so only large banks
- Client Clearing
  - Market participant becomes client of a CCP clearing member
  - Market participant becomes client of a clearing member's client
- At CCP level
  - Omnibus clearing – cheaper but lacks ownership certainty
  - Legally segregated clearing but operationally co-mingled
  - Full asset segregation

EMIR

- European Market Infrastructure Regulation
- Reporting obligation applies to all derivatives (i.e. OTC and exchange-traded)
- Clearing and risk mitigation obligations only to OTC derivatives
- EMIR can apply directly to third country entities
  - Clearing obligation if enter into derivatives subject to clearing obligation with EU derivatives market participants
  - Clearing and collateral exchange apply to derivatives entered into between two offshore parties if contracts have direct, substantial and foreseeable effect in EU
  - Apply to contracts aimed at evading EMIR's rules
  - Non EU party may have to agree to comply with EMIR rules

Non cleared OTC derivatives

- Risk mitigation techniques apply in respect of OTC derivatives that are not cleared via CCPs:
  - Operational risk mitigation techniques
  - Timely confirmation of trades;
  - Daily mark-to-market valuations of trades;
  - Dispute resolution processes in place
  - Engaging in portfolio reconciliation and considering portfolio compression
  - Exchange of collateral
  - Capital requirements for prudentially regulated counterparties

MiFID II - Background

- Markets in Financial Instruments Directive
  - Original MiFID implemented 2007 and still applicable
  - Governs provision of investment services in financial instruments by banks and investment firms and operation of traditional stock exchanges and alternative trading venues
  - Various investor protection measures
- MiFID II
  - Applicable from 3 January 2017
  - Greater regulatory requirements to take account of developments in technology and market infrastructure
  - Enhance investor protection
  - Maximise transparency and reduce data fragmentation

MiFID II – Trading Transparency

- Same pre and post-trade transparency requirements for all venues
- Requirements calibrated for different types of instruments
  - Take into account interests of investors and issuers and government bond issuers
  - Market liquidity
- Requirements calibrated for different types of trading
  - Order-book and quote-driven systems such as request for quote
  - Hybrid and voice broking systems
  - Take account of transaction size / turnover / other relevant criteria

MiFID II – Trading

- Negotiated transactions
  - Volume caps and strict price improvement requirements
  - Limits on negotiated large equities transactions
- Liquidity
  - Disappearance of broker crossing networks for equities
  - Most trades are forced to be executed on trading venues,
  - Prop trading allowed only for bonds on OTF only and restricted to illiquid sovereign debt
  - Restrictive matched principal trading for all bonds & derivatives not subject to the clearing obligation
  - Reduced use of waivers apart from illiquid assets and non equities

MiFIID II - Reporting

- Trading Venues
  - Obligation to maintain records of all orders and all transactions without exemption
- Reporting
  - Obligation to make pre- and post-trade data available separately and in reasonable commercial manner
  - Post trade transparency request reporting as close to real time as possible
  - Daily commodities reporting at national level and weekly to ESMA
- Similar rules apply to Consolidated Tape Providers
  - Must report that computer algorithm by investment firm responsible for the investment decision
  - Must report execution of the transaction or a free information must be made available free of charge max. 15 minutes after publication

Importance of Cyber Security

- Data and security breach has serious operational, financial, legal and reputational implications
- If confidential information, trade secrets or intellectual property are compromised disclosures can seriously damage company's ability to operate
- Cyber-attacks are criminal offence in most countries in Asia
- Types of crime
  - Illegal Access
  - Illegal Interception
  - Misuse of devices
  - Fraud
  - Identity theft

SEC Cybersecurity Sweep

- Written information security policies
  - 93% of broker-dealers
  - 83% of advisers
- Conduct periodic audits to determine compliance with these information security policies and procedures.
  - 89% of broker-dealers
  - 57% of advisers
- Written business continuity plans often address the impact of cyber-attacks or intrusions and mitigating the effects of cybersecurity incident and/or outline the plan to recover from such an incident.
  - 82% for broker-dealers
  - 51% for advisers
- Use of encryption
  - 98% for broker dealers
  - 91% for adviser

SEC Cybersecurity Sweep

- Written policies and procedures generally do not address how firms determine whether they are responsible for client losses associated with cyber incidents.
  - 30% for broker- dealers
  - 13% for advisers
- Offer security guarantees to protect clients against cyber-related losses
  - 15% for broker- dealers
  - 9% for advisers
- Using external standards and other resources to model their information security architecture and processes (epscially NSIT or ISO)
  - 88% for broker dealers
  - 53% for advisers

SEC Cybersecurity Sweep

- Conduct periodic risk assessments, on firm wide basis, to identify cybersecurity threats, vulnerabilities, and potential business consequences
  - 93% for broker-dealers
  - 79% for advisers
- Cybersecurity risk assessments of vendors with access to their networks
  - 84% for broker- dealers
  - 32% for advisers
- 72% of broker-dealers incorporate requirements regarding cybersecurity into vendor contracts but only 24% of advisers
- 58% of brokers have insurance cover but only 21% of advisers
  - Only one insurance claim in both groups

SEC Cybersecurity Sweep

- Firmwide inventory of technology resources
  - Physical devices and systems (96% and 92%)
  - Software platforms and applications (91% and 92%)
  - Network resources, connections, and data flows (97% and 81%)
  - Connections to firm networks from external sources (91% and 74%);
  - Hardware, data, and software (93% and 60%)
  - Logging capabilities and practices (95% and 68%)
- Firm has been subject to a cyber-related incident
  - 88% for broker-dealers
  - 74% for advisers
- Fraudulent emails seeking to transfer client funds
  - 26% of broker-dealers reported losses of more than USD5,000 and biggest was USD75,000
  - Employees not following firms identity authentication procedures

Case Studies - Singapore

- 2013 - Bank statements belonging to hundreds of Standard Chartered's richest customers were found to have been stolen from a server at Fuji Xerox Singapore, the third party where printing was outsourced.
- 2013 - Singapore cyberattacks were a series of attacks initiated by the hacktivist organisation Anonymous, represented by a member known by the online handle "The Messiah". The cyber attacks were partly in response to web censorship regulations in the country, specifically on news outlets.
- 2014 - 317,000 customers of karaoke chain K Box Singapore were posted online by a group of hackers. The group had reportedly sent an e-mail to various media outlets, containing personal information of K Box members including e-mail addresses, contact numbers, NRIC numbers, birth dates, as well as membership details such as the number of loyalty points earned.

MAS's Approach

- Circular on IT Security Risks posed by Personal Mobile Services – September 2014. Requirement for organisations to have policies around data management and access to personal mobile services used at organisations.
- Circular on Vulnerability Assessment and Penetration Testing – May 2014. Requirement to carry out periodic vulnerability and penetration testing on various IT infrastructures.
- Notice on Technology Risk Management - June 2014. Requirement to assess critical IT systems within organisations and inform the MAS when such systems are down.
- Stricter due diligence rules on outsourcing and due diligence on outsourced serviced providers to be released soon.
- Requirement to implement risk management framework which also addresses technology risks.
- Singapore's National Cyber Security Master Plan 2018 aims to strengthen critical technological infrastructure, test the cyber-security readiness of key industry sectors and incorporate cyber-security learning into appropriate higher education courses.
- Singapore's new Cyber Security Agency (CSA) commenced work on 1 April 2015, and oversees this work. The new CSA follows the establishment of an INTERPOL cyber-crime centre in Singapore in 2014.
- Cyber-attacks may constitute an offence under the Computer Misuse and Cybersecurity Act in Singapore.

Contact Information

Hong Kong

ComplianceAsia Consulting Ltd
Suite 502, ChinaChem Tower,
34-37 Connaught Road, Central
Hong Kong
Tel: +852 2868 9070
Fax: + 852 2868 9327

Singapore

ComplianceAsia Consulting Pte Ltd
137 Telok Ayer Street #03-06
Singapore 068602
Tel: +65 6533 8834
Fax: +65 6221 2413

Philippa Allen: philippa.allen@compliancesia.com
Nithi Genesen: nithi.genesen@complianceasia.com

CA | ComplianceAsia