Cyber Security: Regulatory expectations

Regulator	Content/*Observations*
Australian Securities & Investments Commission (ASIC)	• Regulatory Guide 259: Risk Management Systems for Responsible Entities ○ Guidance to fund managers about their risk management systems, including some guidance on cyber resilience ○ It gives specific guidance on how these entities may comply with their obligation under s912A(1)(h) of the Corporations Act 2001 (Corporations Act) to maintain adequate risk management systems • Report 429 (03/2015) on "Cyber resilience: health check": includes a health check list (page 8-14) and relevant legal and compliance requirements for different types of regulated entities (Section D and Appendix 2 **Guides from other Australian agencies:** • Office of the Australian Information Commissioner (OAIC) Guide to securing personal information • OAIC Data breach preparation and response — A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth) • The Australian Signals Directorate Essential Eight Mitigation Strategies and Strategies to Mitigate Cyber Security Incidents – Mitigation Details
Canadian Securities Administrators	• Cyber security is implicitly covered in Part 11 (internal controls and systems) of Regulation 31-103 respecting Registration Requirements, Exemptions and Ongoing Registrant Obligations (c. V-1.1, r. 10) • The Canadian Securities Administrators (CSA) published on 27 September 2016 CSA Staff Notice 11-332 *Cyber Security* to promote cyber-security awareness, preparedness and resilience in Canadian capital markets. The CSA also published on 19 October 2017 CSA Staff Notice 33-321 *Cyber Security and Social Media*, which summarizes survey results of registered firms' cyber security and social media practices, in addition to providing guidance to firms in these areas. • Staff from the British Columbia Securities Commission, the Ontario Securities Commission and the Autorité des marchés financiers published Multilateral Staff Notice 51-347 *Disclosure of cyber security risks and incidents* on 19 January 2017. The notice reports the findings of a review announced by the CSA in Staff Notice *11-332 Cyber Security* and provides disclosure expectations for reporting issuers based on those findings.
EU General Data Protection Directive (GDPR)	• Obligations for data controllers and data processors • Organisational and technical measures to be taken to protect against unauthorised or unlawful access and accidental loss, destruction or damage of data • Notification requirements to regulator

Regulator	Content/*Observations*
FCA Handbook	• SYSC 3 Systems and Controls: focus on establishing and maintaining (1) systems and controls appropriate to the firm's business and (2) risk-centric governance arrangements • SYSC 6.3 Financial Crime: mostly focussed on money laundering and where firms could be used to further financial crime • Principle 3: Management and Control: "…reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems" • Principle 11: Relations with regulators/disclosure: "... deal with regulators in an open and cooperative way" and disclosure to regulators; SUP 15 implies requirement to notify the FCA or PRA of serious cyber security incidents (e.g. SUP 15.3.1 Matters having serious regulatory impact) *Issues relating to cyber security **implicitly** addressed in the FCA Handbook in a principle-based fashion; no dedicated cyber security section.* • Additional FCA Resources on cyber resilience, including publications, and reporting of cyber incidents • Good cyber security – the foundations (1 pager) • *"Our approach to Cyber security in financial services firms"* (speech, 21 September 2016) [Security culture, good governance, identify key assets, protections, detections, recovery/response, information sharing]
International Organization of Securities Commission (IOSCO): Report on IOSCO's cyber risk coordination efforts	The report provides an overview of some of the different regulatory approaches related to cyber security that IOSCO members have implemented thus far. Regulators are generally still in the early stages of developing policy responses in the area of cyber security. The report is organized around the relevant segments of the securities markets, namely: reporting issuers; trading venues; market intermediaries; asset managers; and financial market infrastructures. The report makes numerous references to the SBAI Cyber Security Memo.
Monetary Authority of Singapore (MAS): Technology Risk Management Guidelines and Notice on Technology Risk Management	*Guidelines* • Technology risk management principles and best practices that focus on: ○ Establishing a sound and robust technology risk management framework. ○ Strengthening system security, reliability, resiliency and recoverability. ○ Implementing strong authentication to protect customer data, transactions and systems. *Notice* • Sets out requirements on ○ High reliability, availability and recoverability of critical systems. ○ IT controls to protect customer information from unauthorized access or disclosure. ○ Notification of serious security breaches or failure of critical systems to MAS. *The Cyber Security Agency (CSA) under the Prime Minister's office, coordinates building cyber capabilities and collaborating with the private sector to monitor, detect and mitigate the impact of cyber risks.*

Regulator	Content/*Observations*
National Futures Association (NFA) Self-Examination Questionnaire (02/2016)	• Cyber security questions were added to the NFA Self-Examination Questionnaire • This section is designed to help member firms comply with NFA's Information Systems Security Programs (ISSP) rules and interpretations which came into effect on 1 March 2016
US Securities and Exchange Commission	**Regulation:** • Regulation S-P (adopt written policies and procedures that address administrative, technical, and physical safeguards for the protection of customer records and information) • Regulation S-ID **(**Subpart C): Identity Theft Red Flags; Adopting release • **Compliance Rules (Compliance procedures and practices):** Investment Company Act Rule 38-1, Investment Advisers Act Rule 206(4)-7, Adopting release for ICA Rule 38-1 and IAA Rule 206(4)-7 (see Section II(A)(1) of the Adopting Release, which provides additional information about issues that the policies and procedures of funds or advisers should consider, certain of which are related to cybersecurity) **Engaging Government Agencies and Industry:** • Cybersecurity Guidance for Investment Advisers and Registered Investment Companies (April 2015): ○ Conduct periodic assessment of (1) nature, sensitivity and location of information, … (2) threats to the IT systems, (3) security controls/processes, (4) impact if systems are compromised, (5) effectiveness of governance structure ○ Create strategy to prevent and detect threats ○ Written policies/procedures/training • Guidance on Business Continuity Planning for Registered Investment Companies (June 2016) **Assessing Market Participant Readiness** • OCIE August 2017 – Observations from Cybersecurity Examinations[1] • OCIE May 2017 – Cybersecurity: Ransomware Alert • OCIE September 2015 Cybersecurity Examination Initiative: Particular focus on protection of client information and cyber security-related basic controls (governance and risk assessment, access rights and control, data loss prevention, vendor management, training, incident response). The appendix contains a sample list of materials the OCIE may review • OCIE Summary of 2014 Cybersecurity Examination Sweep: Summary of examination findings of 57 registered broker-dealers and 49 registered investment advisers, focusing on information security policies, business continuity plans, use of external standards (e.g. NIST, ISO or FFIEC frameworks), periodic risk assessments, approach to service providers/vendors, etc. *Provides a good understanding of the OCIE's examination priorities; the program is still being developed/enhanced* • SEC Cybersecurity Roundtable
National Conference of State Legislatures (US)	Overview of security breach notification laws (legislation requiring entities to notify individuals of security breaches of information involving personally identifiable information)

[1] SEC OCIE: Securities and Exchange Commission Office for Compliance Inspections and Examinations

Regulator	Content/*Observations*
Securities and Futures Commission of Hong Kong	• Part IV (Information Management) of "Management, Supervision and Internal Control Guidelines for Persons Licensed by or Registered with the Securities and Futures Commission": policies and procedures are required to be established to ensure integrity, security, availability, reliability and completeness of all information, including documentation and electronically stored data, relevant to the firm's business operation. • Para 18.5 (Adequacy of System) of "Code of Conduct for Persons Licensed by or Registered with the Securities and Futures Commission": also requires that a licensed or registered person should ensure the integrity of the electronic trading system it uses or provides to clients, as may be appropriate in the circumstances, including the system's reliability, security and capacity; firms also should have appropriate contingency measures in place **Circulars:** • Circular dated 11 June 2015 issued to all licensed corporations about launching of an internet trading self-assessment checklist by the Commission. The checklist provides guidance for licensed corporations to conduct regular self-assessment of their internet trading systems, network infrastructure, related policies, procedures and practices in order to identify areas that require improvement and, where needed, enhance the same so to ensure compliance with the relevant electronic trading requirements. • Circular dated 13 Oct 2016 which announced the commencement of a cybersecurity review with a focus on assessing the cybersecurity preparedness, compliance and resilience of brokers' internet/mobile trading systems. • Circular dated 15 May 2017 to all licensed corporations to remind them to be alert for cybersecurity threats (including ransomware attacks) and implement appropriate measures to address the risks. • Two circulars dated 27 Oct 2017 to the licensed corporations engaged in internet trading: ○ Release of the "Guidelines for Reducing and Mitigating Hacking Risks Associated with Internet Trading" which set out 20 baseline preventive, detective and other control requirements for the industry to improve cybersecurity resiliency (minimum standards) ▪ Applies to the following licensed corporations: Type 1 regulated activity (dealing in securities); Type 2 regulated activity (dealing in futures contracts); Type 3 regulated activity (leveraged foreign exchange trading). For the avoidance of doubt, these Guidelines shall only apply to leveraged foreign exchange traders licensed by the SFC; and/or Type 9 regulated activity (asset management) to the extent that they distribute funds under their management through their internet-based trading facilities. ○ Good industry practices for IT risk management and cybersecurity ▪ Senior management, with the help of solution providers or technical consultants if needed, should ensure that all systems and controls are commensurate with the firm's business needs and operations, and implement additional cybersecurity controls as necessary. ▪ List of some good industry practices which internet brokers may wish to consider incorporating into their information technology and cybersecurity risk management frameworks. *Note: The two circulars dated 27 Oct 2017 can apply to fund managers which distribute funds under their management through their internet-based trading*

Regulator	Content/*Observations*
	facilities (as mentioned in Note 2 of the Press Release (http://www.sfc.hk/edistributionWeb/gateway/EN/news-and-announcements/news/doc?refNo=17PR133), " licensed or registered persons engaged in internet trading" refer to licensed or registered persons who, through internet-based trading facilities, are engaged in dealing in securities or futures contracts, in leveraged foreign exchange trading or in distributing funds under management.)
Financial Industry Regulatory Authority (FINRA)	• General Resources, including small firm cyber security checklist (based on NIST cyber security framework and FINRA Report on Cyber Security Practices (02-2015))
Swiss Financial Market Supervisory Authority (FINMA)	• Swiss licensees according to the Swiss Collective Investment Schemes Act (CISA) are required to maintain a proper organisational structure, including risk management, internal control system and compliance according to art. 14 (1 c) in connection with art. 12 and 12a of the Swiss Collective Investment Schemes Ordinance (CISO). In principle this also includes proper processes to deal with cyber risks • Additionally, Swiss licensees must comply with the provisions of the Federal Act on Data Protection (FADP) which aims to protect the privacy and fundamental rights of persons when their data is processed • New guidelines for banks (as of 22 September 2016): *Rundschreiben 2008/21 "Operationelle Risiken – Banken"* (vgl. Rz. 135.6 ff.) • Guidance on IT outsourcing (banks, insurers): see *Rundschreiben 2018/03 Outsourcing Banken und Versicherungen* (vgl. Rz. 24 und 25) • Coverage of Cyber Risk and digitalisation during the 2018 FINMA media conference **National Strategy to protect Switzerland from Cyber Risk 2018-2022 (Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken) (NCS 2018-2022)** ▪ Based on previous version *NCS 2012-2017* and further recommendations (Empfehlungen des *Beirats Zukunft Finanzplatz* vom August 2017) ▪ The strategy defines seven objectives (see page 11 of the NCS 2018-2022) ▪ Next steps: Development of implementation plan national government, Cantons in collaboration with industry) (see press release from Eidgenoessisches Finanzdepartment) *Separately, additional guidance and recommendations have been published by industry associations for the financial sector:* • The Swiss Funds and Asset Management Association (SFAMA) issued its Code of Conduct (CoC), which contains principles with regard to a proper organizational structure (60ff), including an adequate Business Continuity Management (BCM) process (70)