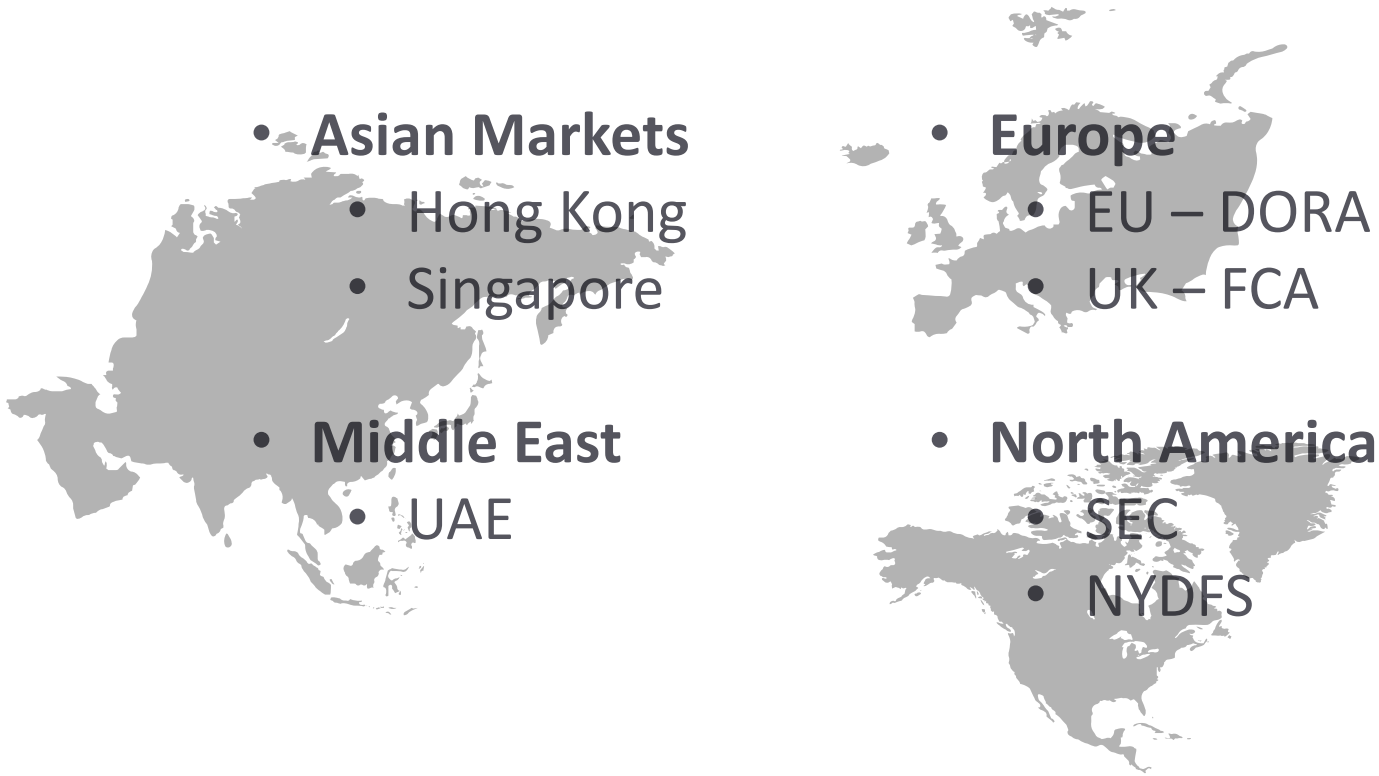
Cybersecurity pressures from LPs and Regulators

Agenda



- **Asian Markets**
  - Hong Kong
  - Singapore
- **Middle East**
  - UAE
- **Europe**
  - EU – DORA
  - UK – FCA
- **North America**
  - SEC
  - NYDFS

Allocators

- DDQ Focus Points
- Internal Trainings

Singapore

Monetary Authority of Singapore

Threat Risk Management Guidelines

- Senior Management Oversight
- Board of Directors approve risk and key decisions with relation to Risk (IT changes)

- Cyber standards for any third parties

- Testing (Pen Testing, Tabletops, Vuln Assess)
- RTO – 4 hours plus notification (severe and widespread impact)
- Independent Audit to assess the effectiveness of controls and risk management.

Hong Kong – Monetary Authority

HONG KONG MONETARY AUTHORITY
香港金融管理局

I. CFI – the goals to be achieved

(i) Adopt a more comprehensive approach for looking at cyber risks

Ok, we know your front door is very secure…

…but what about your backyard?

Hong Kong – Securities and Futures Commission

Focus on Risk Alerts (Circulars)

- Business Email Compromise
- Operational Resilience
- Remote Working
- Instant Messaging
- Ransomware

Key Topics

- Management and Incident Reporting
- Cloud Security
- Remote Access
- Third Party Risks
- Alert List
- “Onsite Inspections”

Ransomware Circular

- Latest Security Patches
- Firewalls
- Offline Backups
- Filter suspicious Emails
- Unmanaged Devices
- Malware protections are updates

United Arab Emirates

Strategy and Framework	Governance and Risk Framework
Risk and Control	Risk Assessment
Governance	Third Party Risk Management
Recovery	Incident Response
Continuous Learning	Awareness Training
Monitoring	Protection Controls
Response	Detection Systems
Information Sharing	Collaboration and Threat Intel

EU DORA

What is DORA?

The Digital Operational Resilience Act (DORA) is an EU regulation that establishes technical standards for nearly all (see: Who does DORA apply to?) financial entities and their critical third-party technology service providers.

When do I need to meet DORA requirements?

The compliance deadline is 17th January, 2025.

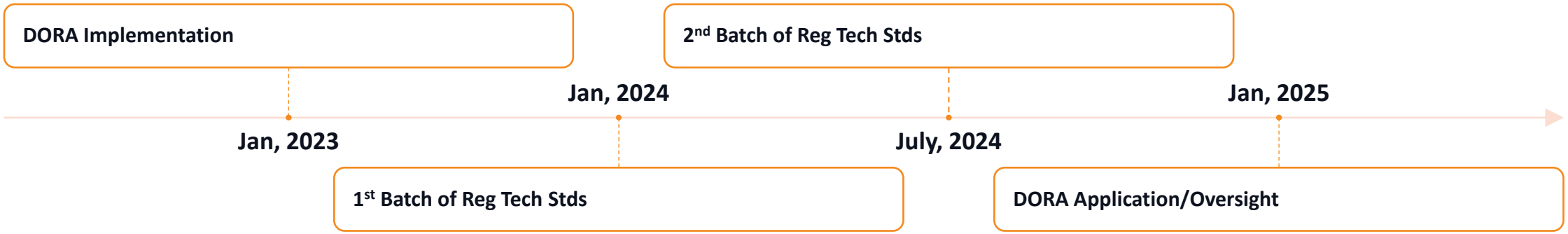
Who does DORA apply to?

The Regulation's scope covers nearly all firms in the financial sector, including managers of alternative investment funds.
It applies to:

- Firms based in the EU
- Firms that operate in the EU
- Firms that invest in funds in the EU

EU DORA – The 5 Pillars

- **ICT risk management -** Set of key principles and requirements on ICT (i.e. digital and data services) independent risk management framework.
- **ICT-related incident reporting -** Harmonise and streamline reporting + extend reporting obligations to all financial entities.
- **Digital operational resilience testing -** Subject financial entities to basic testing or advanced testing (e.g. TLPTs).
- **ICT third-party risk -** Principle-based rules for monitoring third-party risk, key contractual provisions + oversight framework for critical ICT TPPs.
- **Information sharing -** Voluntary exchange of information and intelligence on cyber threats.



DRAWBRIDGE

FCA....

Operational Resilience Requirements

- PRA-designated investment firms
  - Third Party Assessments
  - Scenario Testing (Pen Test, DR Tests, TTX Simulations, etc)
  - Vulnerabilty Management
  - Incident Response Plans

FCA only

SYSC 13.7 - A *firm* should establish and maintain appropriate systems and controls for managing operational risks that can arise from inadequacies or failures in its processes and systems (and, as appropriate, the systems and processes of third party suppliers, agents and others).

SYSC 13.7.8 - A *firm* should ensure the adequacy of the systems and controls used to protect the processing and security of its information, and should have regard to established security standards such as ISO17799

Primer in Cyber at the SEC Cyber

Modern era of Cyber

In 2014 the SEC released Investment Management Guidance specifically targeting Cybersecurity.

The Department of Examinations (previously the OCIE) heavily influenced the requirements.

Release of Risk Alerts

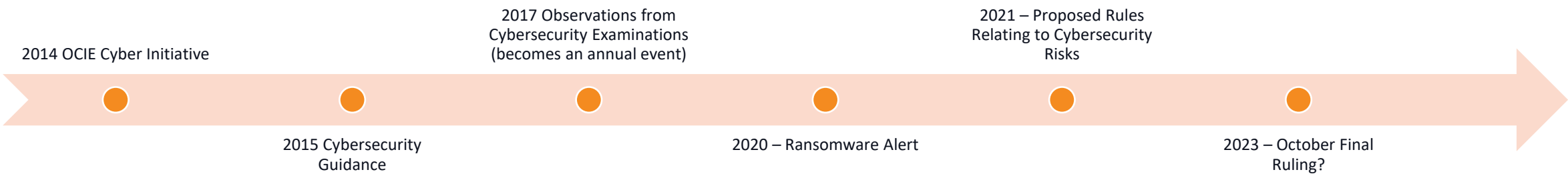
Electronic Messaging, Network Storage, Credential Compromise and most famously - Ransomware.

All are evolutions of the initial guidance and recommendations of Cybersecurity.

Current expectations

- Cybersecurity Policies & Awareness Training
- Incident Response & Business Continuity Planning
- Vulnerability Management,
- Vendor Management,
- Technical Controls - authentication, identification, DLP, email, etc.

Timeline of SEC Rules



NA

What's the Latest from the SEC?

View Rule

View EO 12866 Meetings | Printer-Friendly Version | Download RIN Data in XML

SEC | **RIN:** 3235-AN08 | **Publication ID:** Fall 2023

Title: Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies

Abstract:

The Division is considering recommending that the Commission adopt rules to enhance fund and investment adviser disclosures and governance relating to cybersecurity risks. The Commission proposed new rules to require registered investment advisers ("advisers") and investment companies ("funds") to adopt and implement written cybersecurity policies and procedures reasonably designed to address cybersecurity risks. The Commission also proposed a new rule and form under the Advisers Act to require advisers to report significant cybersecurity incidents affecting the adviser, or its fund or private fund clients, to the Commission. With respect to disclosure, the Commission proposed amendments to various forms regarding the disclosure related to significant cybersecurity risks and cybersecurity incidents that affect advisers and funds and their clients and shareholders. Finally, the Commission proposed new recordkeeping requirements under the Advisers Act and Investment Company Act.

Agency: Securities and Exchange Commission(SEC)
Priority: Substantive, Nonsignificant
RIN Status: Previously published in the Unified Agenda
Agenda Stage of Rulemaking: Final Rule Stage
Major: Undetermined
Unfunded Mandates: No
CFR Citation: 17 CFR 275.206(4)-9 (New) 17 CFR 270.38a-2 (New) 17 CFR 275.204-6 (New)
Legal Authority: 15 U.S.C. 80a-30(a) 15 U.S.C. 80a-37(a) 15 U.S.C. 80b-4 15 U.S.C. 80b-11 15 U.S.C. 80b-3(d) 15 U.S.C. 80b-6(4) 15 U.S.C. 80b-11(a) 15 U.S.C. 80b-11(h) 15 U.S.C. 80a-8 15 U.S.C. 80a-29 15 U.S.C. 80a-37 15 U.S.C. 80b-3(c)(1)
Legal Deadline: None
Timetable:

Action	Date	FR Cite
NPRM	03/09/2022	87 FR 13524
NPRM Comment Period End	04/11/2022	
NPRM Comment Period Reopened	03/21/2023	88 FR- 16921
NPRM Comment Period End	05/22/2023	
Final Action	04/00/2024	

DRAWBRIDGE

2024 Proposed Rule for Investment Companies and Advisers

What can I do now?

- Risk Assessments
- User Security and Access
- Information Protection
- Vulnerability Management
- Written Policies and Procedures
- Incident Response

What are we waiting on?

- Incident Reporting
- Annual Review
- Board Oversight
- Record Keeping
- Prospectus and Brochure Updates

NA

NYDFS

For businesses subject to Part 500, the amendment introduces several new rules to strengthen cybersecurity across the entire business lifecycle, including in business planning, decision-making, and ongoing risk management.

April 2024

- Risk assessments and cybersecurity policies must now be reviewed and updated at least annually.
- Conduct at least annual penetration testing from inside and outside information systems' boundaries.
- Staff training must also occur on an annual basis.

November 2024

- Updated requirements for superintendent notices of cybersecurity incidents.
- Training must be extended to those critical in the implementation of the Incident Response Plan and Disaster Recovery Plan.

May 2025

- Vulnerability management to ensure full coverage over the environment.

November 2025

- Businesses must implement multi-factor authentication (MFA) for all individuals accessing their information systems, including any third-party cloud applications.

What are the Allocators doing around Cyber?

- Teams are more skilled
- DDQ depth
- Benchmarking of Managers
- Pushing the envelope of independence

Wealth management

- 1/5 had cyber measures in place
- 40% have cyber as their top gap risk

THANK YOU

https://www.drawbridgeco.com
info@drawbridgeco.com
US: +1 561-593-1600
UK: +44 (0) 208-078-8825