K&L GATES

Cybersecurity Update

Andrew Gilchrist, Senior Associate, London
Philip Morgan, Partner, London
Sarah Turpin, Partner, London
Cary Meer, Partner, Washington D.C.

Cybersecurity – The current approach of UK and Global Financial Services Regulators

THE APPROACH OF UK AND GLOBAL FINANCIAL SERVICES REGULATORS

- IOSCO Report on Cybersecurity in Securities Markets (April 2016)
  - noted that regulatory approaches tend to be ‘high level’
  - regulators in ‘early stages’ of developing policy responses, in general
  - practices to enhance cybersecurity include (i) effective governance structures involving senior management, (ii) employee training and awareness, including proficiency tests and mock tests, (iii) detection of abnormal patterns of access, (iv) cyber drills and response plans, (v) communication plans, and (vi) information sharing between regulators and market participants

THE APPROACH OF UK AND GLOBAL FINANCIAL SERVICES REGULATORS *(continued)*

- FCA Business Plan 2016/7
  - firms are reliant on complex IT infrastructure making it difficult for them to maintain key services
  - tighter margins lead to more firms outsourcing to third-party firms over which they may have little or no control
  - rigid regulation may stifle innovation
  - overall, FCA expects firms to increase resilience to cyber threats
  - emphasis is less on enforcement, more on helping the industry prepare and encourage sharing of information on best practices, threats etc.
  - no specific focus on cybersecurity in the context of asset managers

THE APPROACH OF UK AND GLOBAL FINANCIAL SERVICES REGULATORS *(continued)*

- Will Brandon – Chief Information Security Officer for the Bank of England – speech 10 May 2016
  - cyber is a ‘clear and present danger’
  - not just a technology problem: people and processes are just as important
  - there needs to be collective corporate will to fix known vulnerabilities
  - weak, default or stolen passwords remain a problem
  - plans need to be rehearsed at all levels
  - it is an identifiable risk that must be managed

Cybersecurity – Developments from Europe

CURRENT POSITION

- Directive 95/46/EC transposed into UK law by the Data Protection Act 1998:

  "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data"

  (Part 1(7), Schedule 1 to DPA) – 7th principle

- Substantial patchwork of laws, including some originating from EU Directives, which can be relevant to cybersecurity issues. These include the Communications Act 2003, the Privacy and Electronic Communications (EC Directive) Regulations 2003, the Computer Misuse Act 1990 and the Official Secrets Act 1989
- Tortious liability - negligence, a breach of confidence or due to misuse of private information
- Contractual liability

WHERE ARE WE HEADING?

- Three important pieces of impending European legislation
- General Data Protection Regulation – in force 23 May 2018
  - Mandatory notification of data breaches to regulator – without undue delay – 72 hours after becoming aware (Article 33) – unless "unlikely to result in risk to rights & freedoms of natural persons
  - Notification to data subjects where "high risk" to rights & freedoms of natural persons (Article 34)
  - Data security standards imposed on "processors" for the first time under statute (Article 32)
  - Increased fines – 2 – 4 % of annual worldwide turnover (or 10,000,000 – 20,000,000 Euros) whichever is higher (Article 83)

WHERE ARE WE HEADING? *(continued)*

- Network and Information Security Directive – expected to be adopted this August (21 month implementation period)
  - Establishes security and notification requirements for certain "operators of essential services" including in banking / financial market infrastructure. UK must identify specific operators within six months of implementation whose operations are critical and will be subject to this regulation
  - Operators must take (1) appropriate and proportionate technical and organisational measures to manage risks; (2) appropriate measures to prevent and minimise impact of incidents / continuity of service; and (3) mandatory notification of incidents having significant impact on continuity of service
  - Operators will be subject to security audits / binding instructions

WHERE ARE WE HEADING? *(continued)*

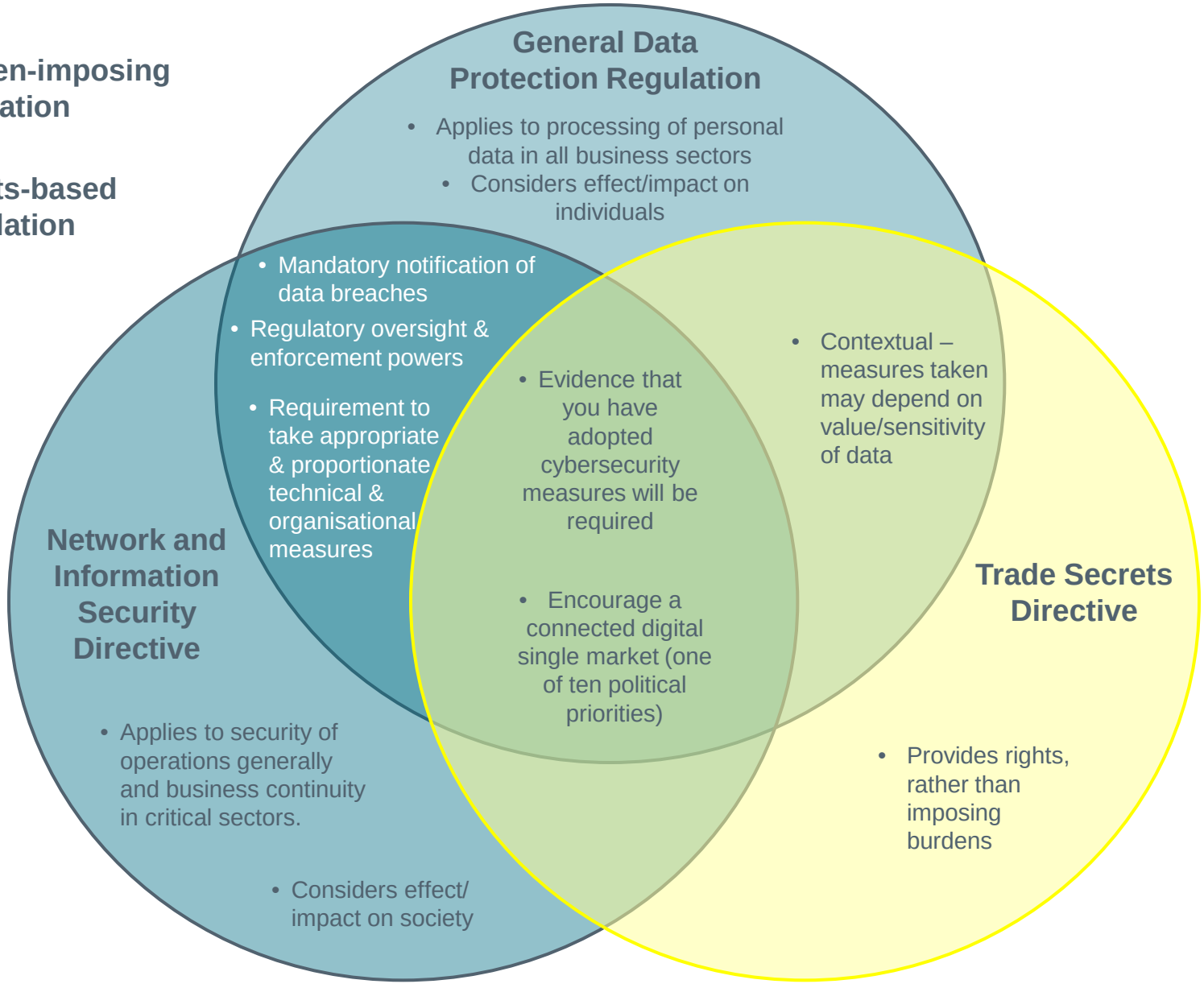
- Trade Secrets Directive – published, backdated to 8 June 2016. 2 Year adoption period
- Creates an enforceable right to protect trade secrets against unauthorised use or disclosure
- One of the criteria for having an enforceable "trade secret":
  - "It has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret"
- What do reasonable steps entail? Similar to US test - "prevent[s] a plaintiff who takes no affirmative measures to prevent its assets from misappropriation, from pursuing trade secret protection"

EUROPE'S DIGITAL SINGLE MARKET STRATEGY

K&L GATES

Burden-imposing legislation

Rights-based legislation



Cyber Insurance

BENEFITS OF CYBER INSURANCE

- Transfer of risk: In the event of a cybersecurity incident, insurance may provide valuable protection for:
  - Claims by third parties seeking damages
  - Notification costs and/or costs for call centres, credit monitoring services, and ID theft monitoring services
  - Cost to investigate and repair computer systems
  - Certain regulatory actions (potentially related to privacy violations, and potentially including certain fines and penalties)
  - Certain business interruption costs (lost profits)
  - Certain extortion threats

Types of Insurance Policies

WHICH INSURANCE POLICIES POTENTIALLY COVER CYBER RISKS?

- Policyholders should consider the unique risks they are facing and carefully review all of their insurance policies to determine the scope of their existing cover and/or the need to purchase additional cyber coverage
- Potential policies at issue:
  - (1) Traditional policies (D&O, E&O/PI, Crime/Fidelity, Property and Business Interruption); and
  - (2) Specialised cyber policies (which may blend various types of policies and/or expand coverage)

WHICH INSURANCE POLICIES POTENTIALLY COVER CYBER RISKS? *(continued)*

- A single cyber event potentially could trigger claims under multiple insurance policies (one event might trigger notification costs and repair costs (Cyber); claims for wrongful acts in providing professional services (E&O/PI); regulatory investigations (E&O/D&O); breach of duty claims (D&O); etc.)

COVERAGE UNDER TRADITIONAL INSURANCE POLICIES – PROPERTY AND BUSINESS INTERPRETATION

- First-party Property policies potentially cover:
  - "Physical damage" to the insured's own property and/or "Loss of use" of "tangible property";
  - Business interruption losses and Extra Expenses arising from covered property damage;
  - Some policies exclude damage to "electronic data" or "loss of use of [or] damage to electronic data." Some cover "electronic data."
- Potential coverage issues:
  - Is "data" stored on a computer "tangible property"?
  - Does damage to electronic data constitute "physical damage"?
  - Whether bits and bytes are "physical" or "tangible" and/or whether the re-arrangement of atoms or molecules on a disc or tape constitutes "direct physical loss"?

TRADITIONAL GENERAL LIABILITY POLICIES

- Third-party policies may cover "personal or advertising injury," which may include "oral, written, or electronic publication of material that violates a person's right of privacy"
- Potential coverage issues:
  - Does the disclosure of confidential information in a public manner constitute a "publication" of material?
  - Who must "publish the material" (Does it cover "publication" by a hacker as opposed to the policyholder itself? Does the policyholder have to intend to "publish"?)?
  - When is there is a "publication" (as soon as material is potentially available to the public or stolen or only if a third party actually reads it)?

PROFESSIONAL INDEMNITY/ERRORS AND OMISSIONS POLICIES

- PI/E&O policies typically only respond where there has been wrongful act / negligence
- Potential coverage issues:
  - Does the policy cover liability of company for deliberate or dishonest acts of employees?
  - Does the cover include claims for libel, slander, invasion of privacy etc?
  - Does the policy exclude liability arising from use of technology / electronic data?

CRIME / FIDELITY POLICIES

- Crime / Fidelity policies typically cover direct loss resulting from theft by employees (or third parties) of money, securities and other tangible property
- Potential coverage issues:
  - Does cover extend to loss or theft of data?
  - Some policies include computer crime extension but may be limited to cost of restoring damaged or corrupted data

D&O POLICIES

- D&O policies may cover potential claims against directors and officers arising from cyber-events, including claims for breach of fiduciary duty
- In the US, there have been a few shareholder lawsuits against directors and/or officers outside of the adviser space. Allegations have included failure to take reasonable steps to protect customer data; failure to maintain industry-standard security protocols; etc.
- To what extent will claims for breach of privacy be followed by claims for breach of duties?

WHAT DO SPECIALIZED CYBER POLICIES COVER?

- There is a rapidly developing market for cyber policies
- The trend is for insurers to develop more specialized forms, but insurers typically are still using policy forms designed for financial institutions generally, rather than specific adviser or fund forms (which are common for D&O and E&O/PI)
- Terms vary widely and insurers are often willing to negotiate to clarify or enhance the cover provided
- Policyholders should focus on attempting to tailor policies to focus on their specific risks and industries
- Policies often blend numerous first-party components and third-party components (policyholder may be able to select among various components)

Overview of Cyber Policies

OVERVIEW OF CYBER POLICIES – FIRST PARTY COVER

- Remediation expenses (may include cost to investigate and repair damage to Computer Systems, including use of forensic experts)
- Notification or crisis management expenses (may include costs incurred under notification laws, credit monitoring, call centres, ID theft monitoring, etc.)
- PR expenses

OVERVIEW OF CYBER POLICY – FIRST PARTY COVER *(continued)*

- Extortion (may be based on threat to introduce malicious code or shut down system; may cover legal expenses, amounts paid, rewards paid; may require cooperation with law enforcement agencies)
- Funds transfer fraud (terms vary widely and may include restrictions)
- Business interruption (lost profits following disruption of service) and extra expense (extra costs incurred to get business running again)

OVERVIEW OF CYBER POLICY – THIRD PARTY COVER

- Privacy and network security (may cover damages and defence costs arising from claims alleging unauthorized access to or dissemination of information, data breaches, transmission of malicious code, denial of service)
- Impaired access (may cover claims arising from insured's systems being unavailable to customers or clients)
- Media liability (claims for libel, slander, invasion of the right of privacy, copyright, trademark, etc.)
- Certain regulatory investigations (may be limited to privacy-related issues, but may expressly cover certain regulatory fines and penalties)

Key issues for Investment Advisers

KEY ISSUES FOR INVESTMENT ADVISERS

- There are heightened risks for advisers/funds given reliance on third-party service providers who may possess the “data” and computer systems
- Coverage varies widely:
  - Some policies may limit coverage to wrongful acts of the insured and/or attacks on the insured’s system
  - Some policies afford coverage with respect to qualified service providers or third party contractors (which may be defined to include third parties the insured hires via a written contract to perform services for the insured)
  - Some policies afford coverage with respect to third parties for whom the insured is “legally responsible”

KEY ISSUES FOR INVESTMENT ADVISERS

(continued)

- Denial of service:
  - In addition to “theft” or “unauthorized use” of data, does policy include denial of service? DDoS generally means attack that restricts or prevents access to computer system
  - Some liability policies afford coverage for a claim against the insured alleging a wrongful act by the insured or qualified service provider resulting in failure to network security. Coverage may turn on activities of insured to protect against unauthorized use, DDoS attacks by a third party, transmission of harmful code, etc.

KEY ISSUES FOR INVESTMENT ADVISERS

(continued)

- Coverage may be limited to “Loss” or “Damages” (may not include fine/penalties)

- Some first-party policies may cover business interruption or extra expense resulting from DDoS attack

KEY ISSUES FOR INVESTMENT ADVISERS

(continued)

- Coverage for fraudulent wire transfers varies widely:
  - Some policies bar coverage for loss arising from the transfer of, or the failure to transfer, funds, money or securities
  - Some policies may cover loss resulting from the insured making payments due to fraudulent input of data into the insured's system or due to fraudulent "instructions." But coverage may be limited to e-mails or faxes, not phone calls or other written advice
  - Coverage may turn on whether insured followed specific procedures (encryption/callback verifications)
  - Some policies may afford coverage for hacks by unauthorized users, but not by authorized users

KEY ISSUES FOR INVESTMENT ADVISERS

(continued)

- Definition of “Data”:
  - Typically includes “Personally Identifiable Information” (definitions vary widely)
  - Does it include employee data?
  - Does it include other types of data, such as proprietary corporate information or trading strategies?

OTHER TERMS OF INTEREST

- Exclusions based on ongoing compliance with standards:
  - Failure to ensure that computer system remained protected by security practices that were disclosed in application for coverage
  - Use of laptops or back-up tapes that do not meet certain encryption standards
  - Use of Wi-Fi networks that do not meet security protocols
  - Use of software that is no longer supported by the third party provider

OTHER TERMS OF INTEREST *(continued)*

- Prior acts exclusions (some polices include broad exclusions based on acts or errors known as of the inception that reasonably could be expected to give rise to a claim)
- Fraud or intentional acts exclusions
  - Is coverage barred only if there is a “final adjudication” in an underlying proceeding?
  - Do you have favourable severability provisions?
- Defence
  - Who controls the defence and/or selects defence counsel?
  - Do you have to choose your lawyers and experts (IT experts, PR firms, call centres, monitoring firms) from a list imposed by insurers?

OTHER TERMS OF INTEREST *(continued)*

- If so, consider negotiating with insurers to facilitate appointment of own choice of legal advisers etc
- “Other insurance” clause (address how multiple policies that might apply to the same risk fit together)

Cybersecurity (U.S.)

K&L GATES

SELECTED U.S. CYBERSECURITY REGULATORY STANDARDS AND DEVELOPMENTS FOR INVESTMENT MANAGEMENT COMPLEXES

2011

- SEC Corporation Finance Disclosure Guidance

2013

- SEC and CFTC adopt Identify Theft Red Flag Rules (Regulation S-ID)

2014

- SEC Roundtable
- OCIE Risk Alert and Sweep Exams
- CFTC Best Practices

2015

- OCIE Risk Alert and Sweep Exam Summary
- FINRA Report on Cybersecurity Practices
- IM Guidance Update
- NFA Cybersecurity Guidance
- Second OCIE Risk Alert
- Second Round of OCIE Sweep Exams
- SEC Enforcement

2016 and Future Initiatives

- More Enforcement
- More Examinations
- More Interpretive Guidance?
- More Rulemaking?

Primary Legal Requirements:

- Regulation S-P (Safeguards Rule)
- Regulation S-ID (Identity Theft Red Flags)
- IAA Rule 206(4)-7 (Compliance Rule)
- IAA Rule 204-2(g) (Electronic Recordkeeping Rule)
- NFA Cybersecuirty Guidance
- Disclosure considerations
- Business continuity plans
- Suspicious activity reporting
- CFTC Regulations, Part 160.30
- FTC enforcement of Section 5 of FTCA
- State data breach and information security program requirements

Primary Regulatory Authorities:

- Securities and Exchange Commission
- Financial Industry Regulatory Authority
- Commodity Futures Trading Commission
- National Futures Association
- Federal Trade Commission
- Banking Regulators (Fed, OCC)
- Federal and State Enforcement Authorities

IM GUIDANCE UPDATE (APRIL 28, 2015)

- SEC staff identified a number of measures that advisers and funds may wish to consider in addressing cybersecurity risk, including:
  - Conduct a periodic assessment of: (1) the information held and systems used by the firm; (2) threats and vulnerabilities; (3) existing controls; (4) potential impact of an incident; and (5) the cybersecurity governance structure
  - Create a strategy designed to prevent, detect and respond to threats, which may include: (1) access and technical network controls; (2) encryption; (3) restricting use of removable storage media and deploying software that monitors for threats and incidents; (4) data backup and retrieval; and (5) the development of an incident response plan. Routine testing of strategies could also enhance the effectiveness of any strategy
  - Implement the strategy through written policies and procedures and training

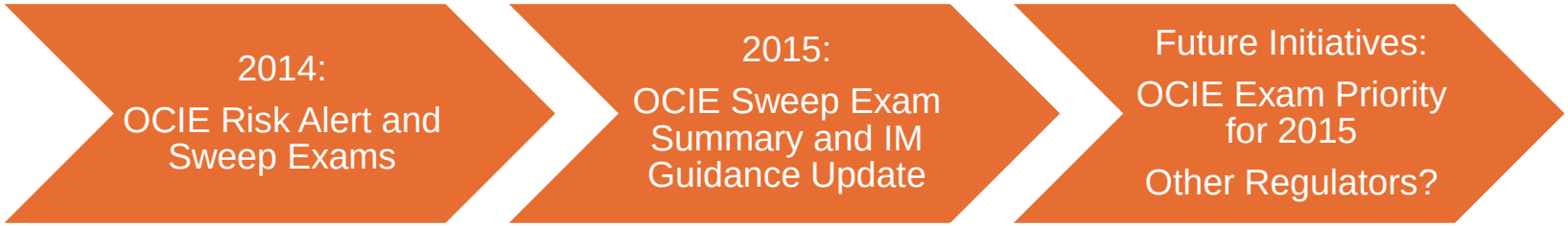
IM GUIDANCE UPDATE *(continued)*

- Potential implications for compliance programs and regulatory risk exposure:
  - "In the staff's view, funds and advisers should identify their respective compliance obligations under the federal securities laws and take into account these obligations when assessing their ability to prevent, detect and respond to cyber attacks….[F]unds and advisers may wish to consider reviewing their operations and compliance programs and assess whether they have measures in place that are designed to mitigate their exposure to cybersecurity risk"
  - Staff stated that compliance policies and procedures could address cybersecurity risks relating to identity theft and data protection (Regulations S-P and S-ID), business continuity, and fraud (Codes of Ethics – insider threats), "as well as other disruptions in service that could affect, for instance, a fund's ability to process shareholder transactions" (Section 22(e) and Rule 22c-1)

COMPLIANCE PROGRAM REQUIREMENTS

- IAA Rule 206(4)-7 requires registered investment advisers to (1) designate a chief compliance officer ("CCO"), (2) adopt and implement written policies and procedures reasonably designed to prevent violation of the federal securities laws, and (3) review annually the adequacy and effectiveness of such policies and procedures
- Cybersecurity compliance policies and procedures that address requirements under the federal securities laws should be included in compliance programs and evaluated as part of the annual review, which should include risk assessments, policy and procedure reviews, and service provider reviews

SEC CYBERSECURITY SWEEP EXAMINATIONS



- SEC Sweep Exam Findings on CCO Involvement in Cybersecurity
  - Significant majority of advisory firms assign information security responsibilities to Chief Technology Officers or to other senior officers, including Chief Compliance Officers, to liaise with third-party consultants who are responsible for cybersecurity
  - Less than a third of the examined advisers (30%) have a Chief Information Security Officer

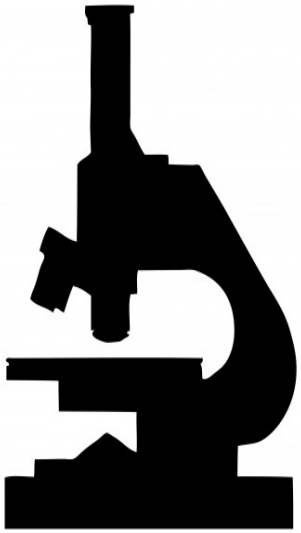
SEC CYBERSECURITY SWEEP EXAM INITIATIVE

- The SEC's Office of Compliance, Inspections and Examinations examined 49 registered investment advisers and 57 registered broker-dealers in 2014 as part of its Cybersecurity Exam Initiative and issued a Risk Alert summarizing its observations in January 2015. Primary observations included:

- ✓ Most advisers (74%) reported that they have been the subject of a cyber-related incident
- ✓ The vast majority of examined advisers (83%) have adopted written information security policies, and over half of them (57%) audit compliance with these policies
- ✓ A high percentage of examined advisers report conducting firm-wide inventorying, cataloging or mapping of their technology resources
- ✓ The vast majority of the examined advisers conduct periodic risk assessments
- ✓ Almost all of the examined advisers (91%) made use of encryption in some form
- ✓ Approximately half of the examined advisers (53%) are using external standards and other resources to model their information security architecture and processes
- ✓ Approximately a third (32%) of the examined advisers require risk assessments of vendors with access to their networks
- ✓ Approximately a quarter of examined advisers (24%) include cybersecurity requirements in contracts with vendors
- ✓ Approximately a third of the examined advisers (30%) have an individual assigned as the firm's Chief Information Security Officer
- ✓ Written business continuity plans often address the impact of cyber attacks or intrusions, but only about half (51%) of adviser policies discuss mitigating cybersecurity incidents
- ✓ Approximately a quarter of examined advisers (21%) maintain insurance that covers losses and expenses from cybersecurity incidents

THE 2014 SEC CYBERSECURITY SWEEP EXAM TOPICS

- The 2014 Sweep focused on the following six topics:



- Identification of Risks/Cybersecurity Governance
- Protection of Firm Networks and Information
- Risks Associated with Remote Customer Access and Funds Transfer Requests
- Risks Associated with Vendors and Other 3rd Parties
- Detection of Unauthorized Activity and
- Experience with Cybersecurity Attacks (network breach, malware, fraudulent transfer requests, etc.)

OCIE 2015 RISK ALERT/ 2015 CYBERSECURITY EXAMINATION FOCUS

- Focus on cybersecurity-related controls and implementation testing:
  - Governance and risk assessment
  - Access rights and controls
  - Data loss prevention
  - Vendor management
  - Training
  - Incident response

CCO PLANNING ITEMS

1. Conduct cybersecurity risk assessment
2. Incorporate cybersecurity compliance risks into the firm's risk matrix
3. Review adequacy of policies and procedures, including those relating to cybersecurity requirements
4. Assess the effectiveness of implementation of the firm's cybersecurity policies and procedures, including testing
5. Due diligence on third party vendors
6. Incorporate cybersecurity into annual review of compliance program
7. Incident response planning

NFA CYBERSECURITY GUIDANCE

- Effective March 1, 2016
- Applies to registered CPOs and CTAs

NFA CYBERSECUITY GUIDANCE *(continued)*

- Elements:
  - Written information systems security program
  - Approval by CEO, CTO or other executive
  - Reports to board
  - Annual review
  - Can be enterprise-wide
  - Security and risk assessment
  - Document and describe safeguards
  - Incident response plans
  - Training
  - Third-party service providers
  - Recordkeeping

TESTING CONSIDERATIONS

- Testing – Important aspect of assessing compliance programs
  - Firms routinely conduct testing as part of annual assessment
  - OCIE and the NFA routinely ask for information about testing results in connection with inspections
- Common types of compliance testing:
  - Transactional Tests – Transaction-by-transaction tests conducted contemporaneously with the transaction
  - Periodic Tests – Transaction-by-transaction tests performed on a “look back” basis at relevant intervals, such a spot checks or random or regular detailed reviews
  - Forensic Tests – Tests that analyze data over a period of time looking for trends and patterns
- Traditional tests can be used in cybersecurity area (e.g., testing privilege management, document destruction, authentication procedures, red flag identification/response, physical safeguards)

SEC 2015 ENFORCEMENT CASE

- Firm failed to adopt cybersecurity policies and procedures
- Breach compromised personally identifiable information for 100,000 individuals
- Censure and $75,000 penalty
- No client harm suffered and firm responded after breach

K&L GATES