

CYBER SECURITY

Taming the Lion

Session 3a

Karen Steighner

Compliance Advisers, Inc.

ksteighner@complianceadvisers.com

303-795-0400

Philip A. Feigin

Lewis Roca Rothgerber Christie LLP

pfeigin@lrrc.com

303-628-9509

Agenda

- Defining Cybersecurity and its Evolution
- Practical Guidance for Cybersecurity
- What programs and software are available to detect cybersecurity breaches
- The role of compliance regarding cybersecurity
- Important elements to be included in a cybersecurity program – policies, procedures, and oversight processes

Defining *Cybersecurity*

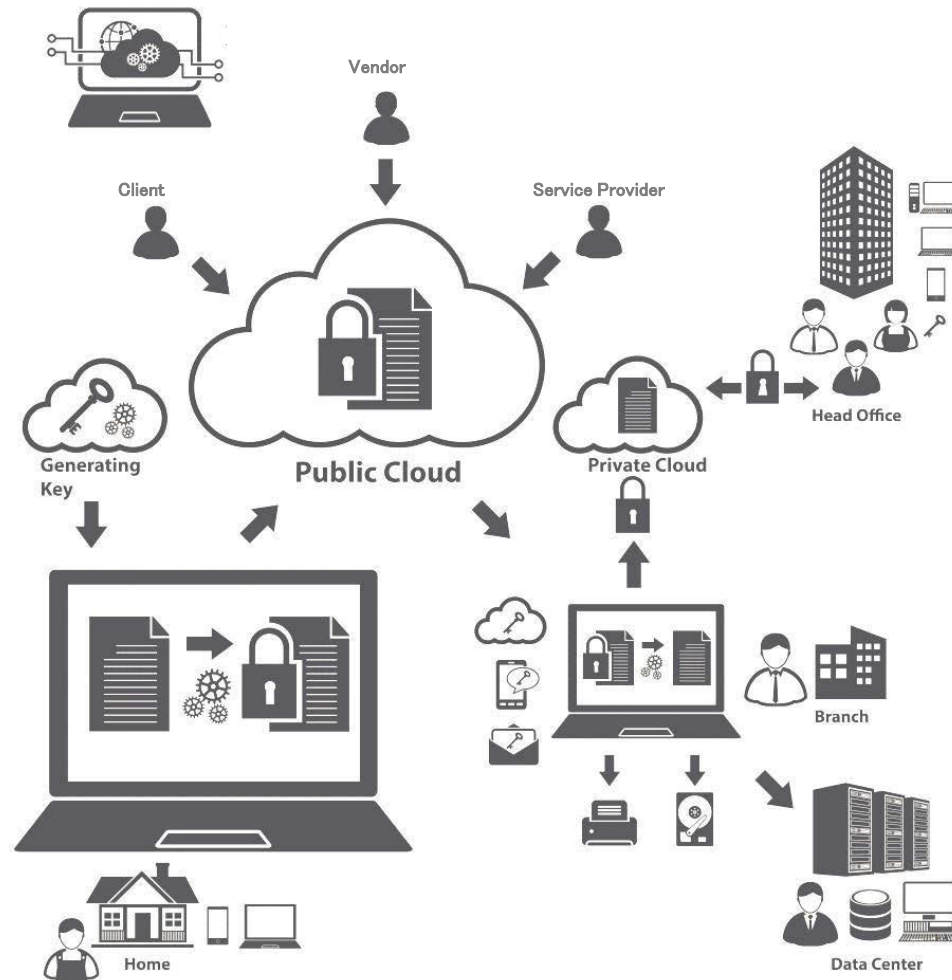
- **FINRA:** “The protection of investor and firm information from compromise through the use—in whole or in part—of electronic digital media (e.g., computers, mobile devices or Internet protocol-based telephony systems).”
- “**Compromise**” refers to a loss of data confidentiality, integrity or availability.
- May overlap with anti-fraud efforts (e.g. socially engineered phishing attacks)

Double Trouble





Cybersecurity poses a **double threat** to regulated firms—

- **Threat of a cyber breach** and all that follows
- **Threat of regulators** finding the firm's written policies and procedures for dealing with cybersecurity are missing or inadequate, *even if* there has been no cyber attack and *even if* there has been no customer harm

Who, How, What & Where?



CHEW-Criminal-Hactivist-Espionage-War

	CRIMINAL	HACTIVIST	ESPIONAGE	WAR
				
Definition	Organized groups of criminals who hide in "cyber sanctuary" countries to launch broad based attacks against individuals and companies for financial gain.	Loosely organized collections of hackers launching targeted campaigns against specific entities or web sites and able to cause embarrassment and financial damage.	Cyber espionage operations are largely carried out by nation-states are extremely well-organized and well-funded. They use this stolen intellectual property to enhance their own economies.	This is when the motivations of a nation-state or a terrorist group turn from intellectual property theft towards damage and destruction.
Motivation	<ul style="list-style-type: none"> • Money • Information to sell (e.g. credit card numbers) 	<ul style="list-style-type: none"> • Protest • Revenge • Demonstration of power 	<ul style="list-style-type: none"> • Acquiring secrets • National security • Economic benefit 	<ul style="list-style-type: none"> • Destroy, degrade, deny • Political motivation
Capability	<ul style="list-style-type: none"> • Large number of • Basic to Advanced skills • Present in nearly all countries 	<ul style="list-style-type: none"> • Large number of • Tend to have limited skills • Few with advanced skill sets and motivations 	<ul style="list-style-type: none"> • Small but growing countries with capability • Larger array of 'support' 	<ul style="list-style-type: none"> • Limited number of • Potential non-state actors • Expensive to maintain

Sweeps, Surveys & Initiatives

FINRA
A REPORT FROM
THE FINANCIAL INDUSTRY REGULATORY AUTHORITY

Report on Cybersecurity Practices

FEBRUARY 2015

Contents	
Executive Summary	1
Background	3
Governance and Risk Management for Cybersecurity	6
Cybersecurity Risk Assessment	12
Technical Controls	16
Incident Response Planning	23
Vendor Management	26
Staff Training	31
Cyber Intelligence and Information Sharing	34
Cyber Insurance	37
Conclusion	38
Appendix I – Summary of Principles and Effective Practices	39
Appendix II – The NIST Framework	42
Appendix III – Encryption Considerations	45
Endnotes	46

REPORT ON CYBERSECURITY PRACTICES—FEBRUARY 2015

NATIONAL EXAM PROGRAM
RISK ALERT

By the Office of Compliance Inspections and Examinations ("OCIE")
Volume IV, Issue 4
February 3, 2015

CYBERSECURITY EXAMINATION SWEEP SUMMARY

I. Introduction

OCIE's National Examination Program staff (the "Staff"), recently examined 57 registered broker-dealers and 49 registered investment advisers to better understand how broker-dealers and advisers address the legal, regulatory, and compliance issues associated with the "Cybersecurity Examination Initiative" or the "Initiative".² The examined firms' vulnerability to cyber-attacks. Appendices A and B include the types of broker-dealers and advisers examined.

The staff collected and analyzed information from the selected firms relating to: identifying risks related to cybersecurity; establishing cybersecurity policies, procedures, and oversight processes; protecting firm networks; identifying and addressing risks associated with remote access to client funds transfer requests; identifying and addressing risks associated with reviews with key personnel at each firm regarding its: business and operations; detecting unauthorized activity. In addition to reviewing with vendors of cyber-attacks; preparedness for cyber-attacks; training and policies; and protocol for reporting cyber breaches.³

The reviews and questions were designed to discern basic distinctions among the examined firms. The staff conducted limited testing of the examined firms are those of the staff of OCIE, in coordination with other staff of the Securities and Exchange Commission ("SEC" or "Commission"), including the Division of Trading and Markets and the Division of Investment Management. The Commission has expressed no view on the contents of this Risk Alert. This document was prepared by the SEC staff and is not legal advice.

The "Cybersecurity Examination Initiative" (April 15, 2014), available at: [http://www.sec.gov/ocie/2014/04/15/14.pdf](#).
The period for broker-dealers covered calendar year 2013; adviser examinations, which included the broker-dealer examinations, reviewed firm practices in 2013 through April 2014.

Compilation of Results of a Pilot Survey of Cybersecurity Practices of Small and Mid-Sized Investment Adviser Firms

North American Securities Administrators Association
www.nasaa.org

OCIE & FINRA Sweep Exams Focus

- Cybersecurity risk identification, governance and risk management practices;
- Cybersecurity policies & procedures and Oversight
- Cybersecurity risk assessments,
- Protection of networks and firm information
- Remote access to client information and fund transfer requests;
- Oversight of third-party vendors
- Protection against unauthorized activity

Sweep Results

Top Three Perceived Threats

- **Hackers** penetrating systems for the purpose of account manipulation, defacement or data destruction, for example
- **Operational risk associated with environmental problems** (e.g. power failures) or natural disasters (e.g. earthquakes, hurricanes)
- **Unauthorized Access** – Employees or other authorized users abusing their access by harvesting sensitive information or otherwise manipulating the system or data undetected

2016 OCIE Priorities

- **In September 2015, second initiative to examine broker-dealers' and investment advisers' cybersecurity compliance and controls.**
- **In 2016, SEC will advance its efforts to assess and test firms' implementation of procedures and controls.**

Regulatory & Legal Actions

- *In the Matter of R.T. Jones Capital Equities Management, Inc.*
- *Dwolla, Inc.*

Practical Guidance for Cybersecurity

SEC Regulation S-ID (the “Identity Theft Red Flag Rule”)

- Applies to “financial institutions” holding transaction accounts
- Requires adoption of reasonable policies and procedures designed to prevent and detect identity theft
- Includes detailed guidelines to develop the firm’s Identity Theft Prevention Program
- Periodic program review and updating

Cost of a Cybersecurity Data Breach

Ponemon Institute Study

Direct Costs

- Detection or Discovery
- Escalation
- Notification
- Post Data Breach

Indirect Costs

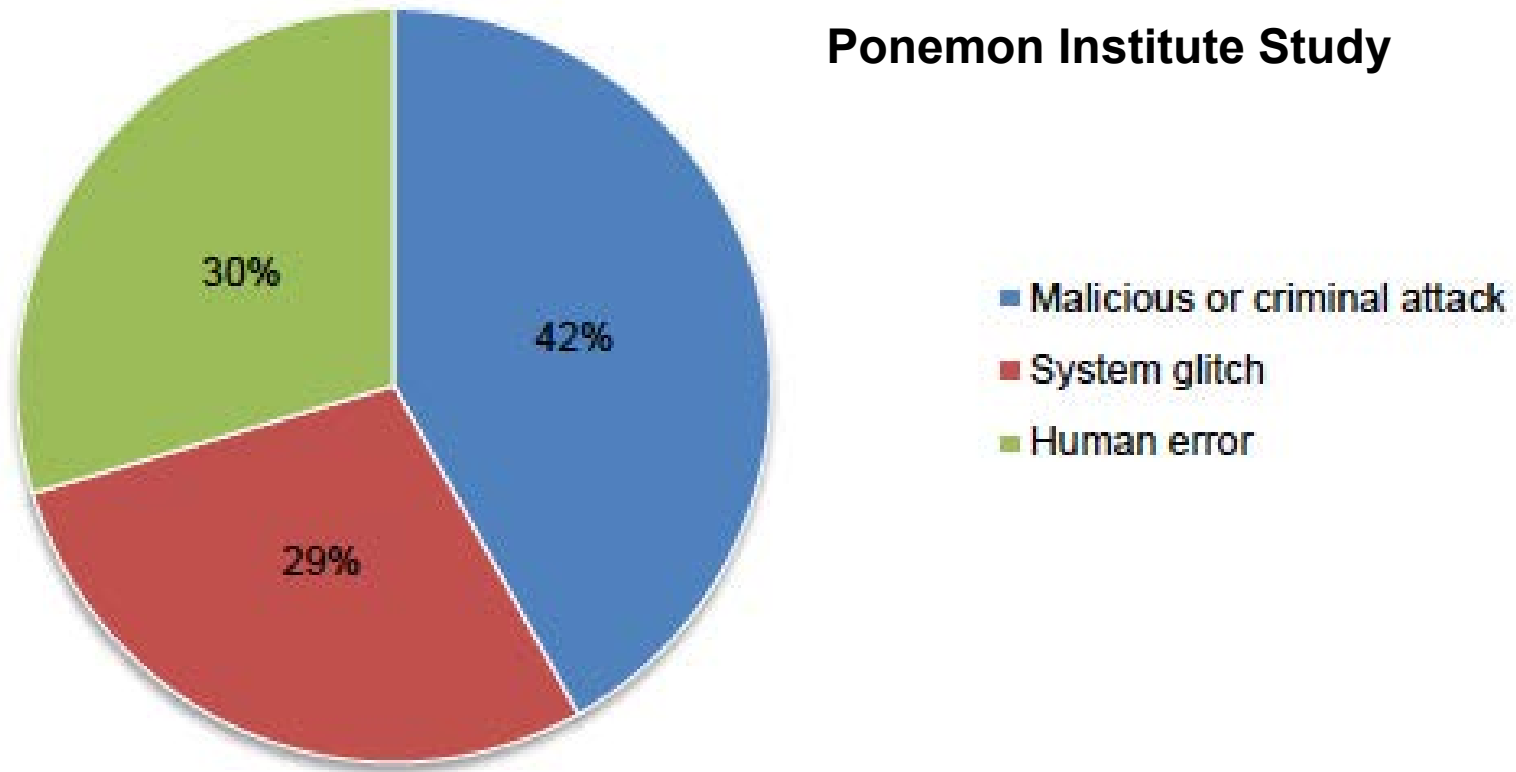
- Turnover of Existing Customers
- Diminished New Customer Acquisitions

Average U.S. Data Breach Costs

Ponemon Institute Study

- Average Per Capita Cost Over Two Years: **\$188**
- Per Capita Costs For Financial Industry: **\$206**
- Data Breach Notification Laws Impact Notification Costs: Avg **\$509K**
- Lost Business Cost: Average **\$3.3 Million**
- Post data breach costs: Average **\$1.6 Million**

Causes of Cybersecurity Data Breach



Practical Cybersecurity Guidance for Compliance

FINRA Cybersecurity Guidance

Practical Cybersecurity Guidance for Compliance

- **Governance and Risk Management**
- **Cybersecurity Risk Assessment**
- **Technical Controls**
- **Incidence Response Planning**
- **Vendor Management**
- **Staff Training**
- **Cyber Intelligence and Information Sharing**
- **Cyber Insurance**

Practical Cybersecurity Guidance

➤ Governance and Risk Management

Practical Cybersecurity Guidance

Governance & Risk Management

➤ Governance Framework

- Active executive management and board-level leadership
- Evaluate & select framework and standards options
- Use metrics and thresholds
- Dedicate resources
- Ongoing, regular Cybersecurity risk assessments

Practical Cybersecurity Guidance

Governance & Risk Management - Frameworks Cybersecurity Frameworks & Standards Options

- The NIST Framework
- ISO
- The SANS Top 20 CIS Critical Security Controls
- IEC
- ISACA's **COBIT**

Practical Cybersecurity Guidance

Governance & Risk Management - Frameworks

The NIST Framework

- Core
 - Identify, Protect, Detect, Respond, Recover
- Implementation Tiers
 - Partial, Risk Informed, Repeatable, Adaptive
- Profile
 - Current State of Cybersecurity Preparedness

Practical Cybersecurity Guidance

Governance & Risk Management - Frameworks

Sans Top 20 Critical Security Controls

- Recommended set of actions for cyber defense
- Specific and Actionable
- Prioritize Fewer Actions with High Payoff
- Derived from the Most Common Attack Patterns
- Transform “Best-in-Class Threat Data into Actionable Guidance

Practical Cybersecurity Guidance

Governance & Risk Management - Frameworks

Metrics

- Provide Visibility on Performance
- Define Target Performance Levels
- Facilitate Decision-Making
- Allocation of Resources

Practical Cybersecurity Guidance

- **Governance and Risk Management**
- **Cybersecurity Risk Assessment**

Practical Cybersecurity Guidance

Cybersecurity Risk Assessment

Risk Assessment Activities—

- Identify and document asset vulnerabilities;
- Review threat and vulnerability information from information sharing forums and sources;
- Identify and document internal and external threats;
- Identify potential business impacts and likelihoods;
- Use threats, vulnerabilities, likelihoods and impacts to determine risk; and
- Identify and prioritize risk responses...

Practical Cybersecurity Guidance

Cybersecurity Risk Assessment

...Create Controls to Remediate Identified Risks

- Preventive
- Detective
- Corrective
- Predictive

Practical Cybersecurity Guidance

Cybersecurity Risk Assessment

Impacts

Actors

Prioritizing Threats

	Regulatory	Reputation Damage	Financial Theft	Intellectual Property Theft	Destruction of critical assets	Business Disruption	Threats to life / safety
Insiders							
Third Parties							
Hacktivists							
Skilled Individual hackers							
Organized Criminals							
Nation-States							

- Deloitte Center for Financial Services analysis

Practical Cybersecurity Guidance

Cybersecurity Risk Assessment

Risk Assessment Sample

#	Critical Asset	Type of attack to which asset is most vulnerable	Data Classification	Exposure	Probability of Occurrence	Impact	Risk	Mitigation
1	Firm's Customer Relationship Management System*	1. Theft of or Unauthorized Access to Personally Identifiable Information (PII) 2. DDOS Attacks 3. Website Defacement	Highly Confidential	External	High	High	1. Business Disruption 2. Reputational Risk 3. Financial Loss	1. Use of SSL 2. Multi layered authentication
2	Firm's Trading Platform*	1. DDOS Attacks 2. Unauthorized access by firm's employee	Highly Confidential	Internal and External	Medium	High	1. Business Disruption 2. Financial Loss due to acts intended to	1. Multi layered authentication 2. Inventory system access

Practical Cybersecurity Guidance

- **Governance and Risk Management**
- **Cybersecurity Risk Assessment**
- **Technical Controls**

Practical Cybersecurity Guidance

➤ Technical Controls

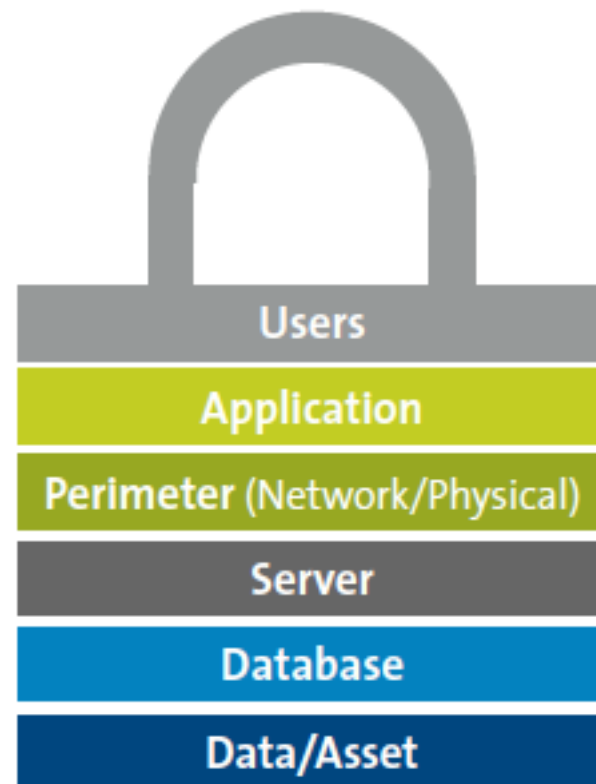
- Implement a “defense-in-depth” strategy (layered security)
- Select controls appropriate to the firm’s technology and threat environment

Practical Cybersecurity Guidance

Technical Controls

In-Depth Defense Measures

- Usernames & Passwords
- Access Controls
- Application Whitelisting
- Virus & Spam Filters
- Secure Operating Systems
- Software Updates
- Back Ups
- Security & Data Encryption



Practical Cybersecurity Guidance

Technical Controls

Programs and Software

- Username & Password Protection Software
- Control Admin Privilege Software
- Application Whitelisting
- Spam Filters
- Secure, Standard Operating Systems
- Analysis
- Vulnerability Scanning & Management
- Secure Application Development
- Forensic Testing Tools
- Backup Tools

- Network Security

Practical Cybersecurity Guidance

- **Governance and Risk Management**
- **Cybersecurity Risk Assessment**
- **Technical Controls**
- **Incidence Response Planning**

Practical Cybersecurity Guidance

➤ Incident Response Planning

- Containment & Mitigation
- Eradication & Recovery
- Investigation
- Notification
- Making Customers Whole

Practical Cybersecurity Guidance

Incidence Response Planning

Effective Practices

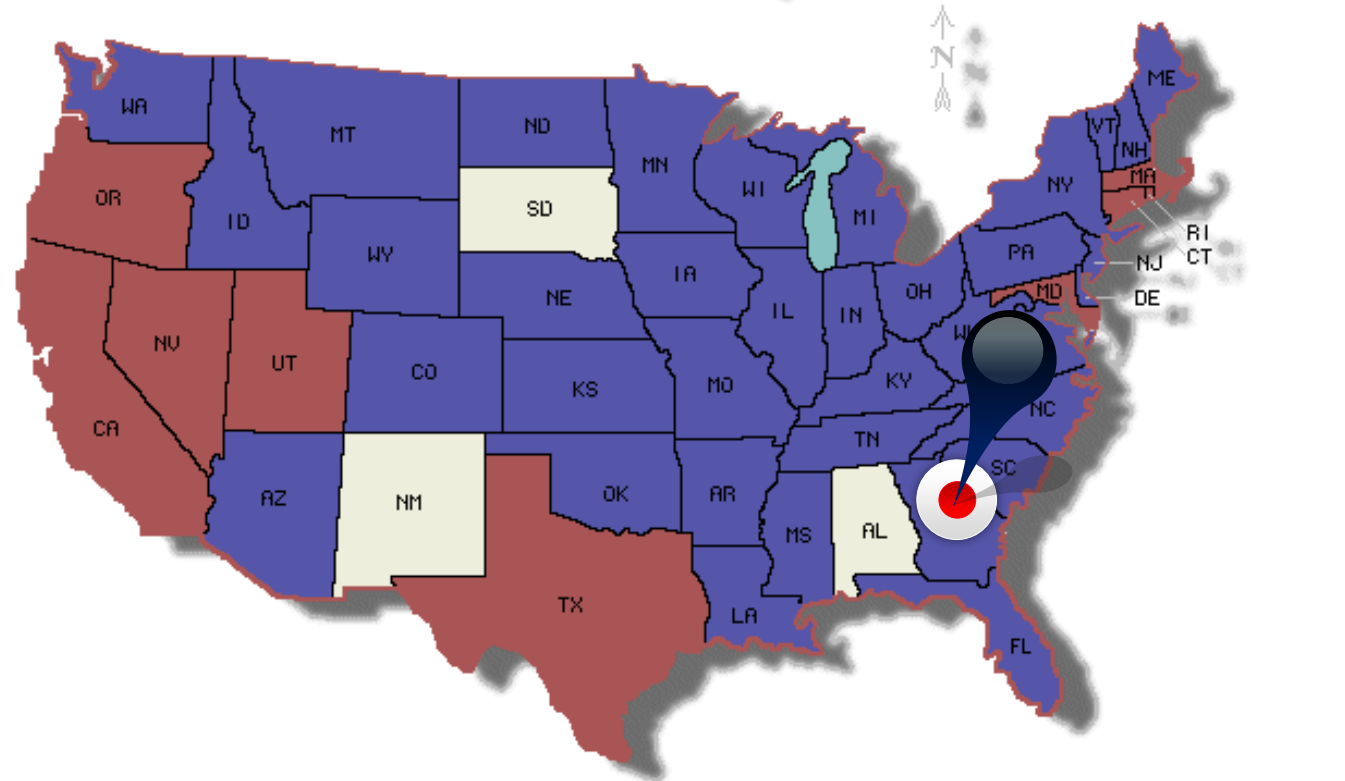
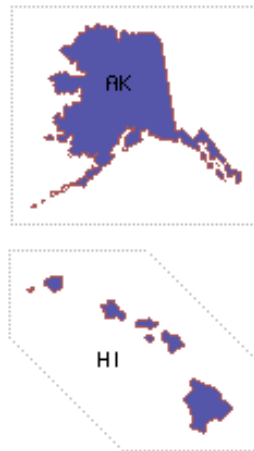
- Prepare Firm Specific Responses
- Incorporate Current Threat Intelligence
- Develop Containment and Mitigation Strategies
- Adopt Eradication and Recovery Plans
- Develop Investigation and Damage Assessment Processes
- Prepare Communication/Notification Plans for Outreach to Relevant Stakeholders
- Industry-wide, Firm-specific Simulation Exercises
- Client Confidence Measures & Loss Reimbursement

Practical Cybersecurity Guidance

Incidence Response Planning

- - Data Security Law
- - Data Breach Law
- - No Law

State and Foreign Privacy Laws



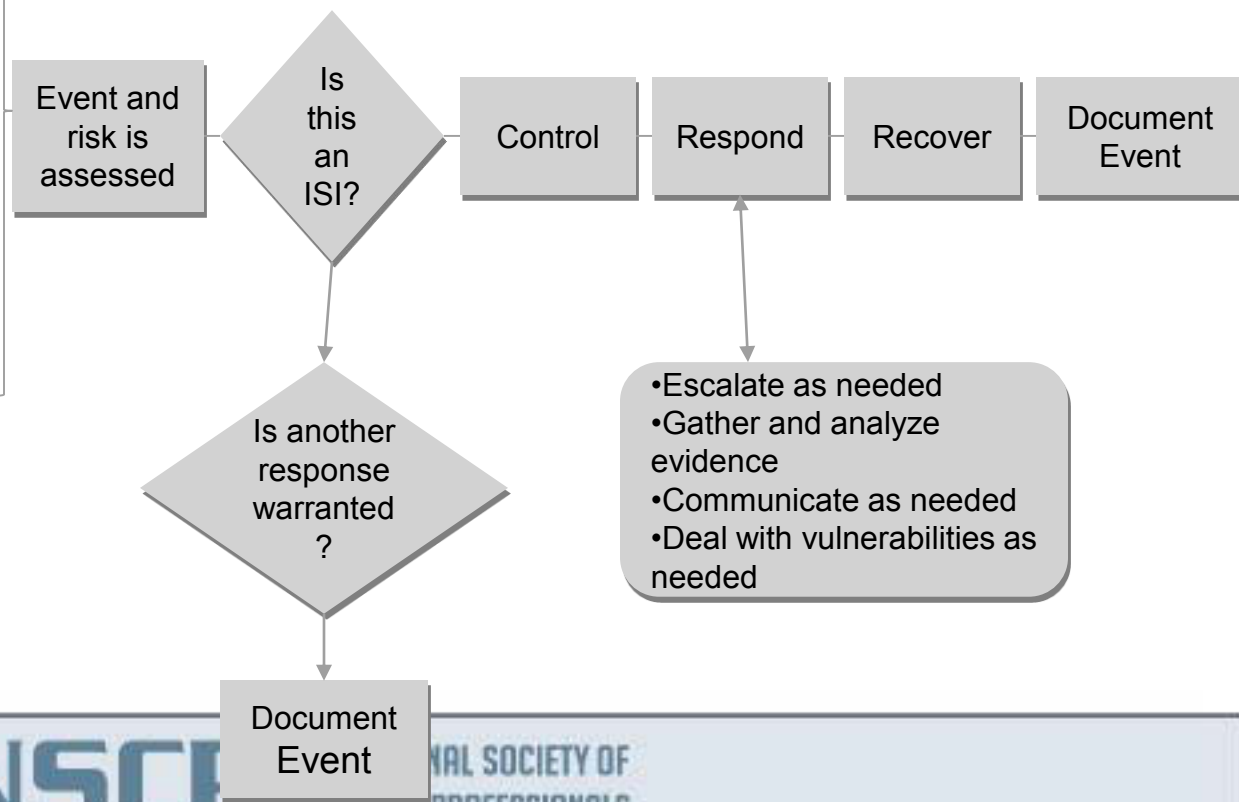
Practical Cybersecurity Guidance

Incidence Response Planning

Plan and Prepare	Detect and Report	Access and Decide	Respond	Lessons Learned
------------------	-------------------	-------------------	---------	-----------------

Polices & Procedures	Controls detect an event
Log & Report Management	Monitoring detects an event
Planning & Testing	Vulnerability is detected
Awareness & Training	Event is reported
Vulnerability Assessment	Vulnerability is identified

Example Response System



Practical Cybersecurity Guidance

- **Governance and Risk Management**
- **Cybersecurity Risk Assessment**
- **Technical Controls**
- **Incidence Response Planning**
- **Vendor Management**

Practical Cybersecurity Guidance

➤ Vendor Management

- Perform pre-contract due diligence on prospective service providers
- Establish appropriate contractual terms
- Perform ongoing due diligence on existing vendors
- Include vendor relationships and outsourced systems as part of the firm's ongoing risk assessment process
- Establish and implement vendor termination procedures
- Establish, maintain and monitor vendor entitlements

Practical Cybersecurity Guidance

Vendor Management

Contractual Provisions

- Legal Team
- Due Diligence Teams
- Custodians of Contract Language
- Standardized Language

Practical Cybersecurity Guidance

- **Governance and Risk Management**
- **Cybersecurity Risk Assessment**
- **Technical Controls**
- **Incidence Response Planning**
- **Vendor Management**
- **Staff Training**

Practical Cybersecurity Guidance

➤ Staff Training

- Define Cybersecurity Training Needs Requirements
- Identify Appropriate Cybersecurity Training Update Cycles
- Deliver Interactive Training with Audience Participation to Increase Retention
- Develop Training Around Information from the Firm's Loss Incidents, Risk Assessment Process and Threat Intelligence Gathering

Practical Cybersecurity Guidance

- **Governance and Risk Management**
- **Cybersecurity Risk Assessment**
- **Technical Controls**
- **Incidence Response Planning**
- **Vendor Management**
- **Staff Training**
- **Cyber Intelligence and Information Sharing**

Practical Cybersecurity Guidance

➤ Cyber Intelligence and Information Sharing

- Assign responsibility
- Establish mechanisms to disseminate threat intelligence and analysis rapidly to appropriate groups within the firm
- Evaluate threat intelligence from tactical and strategic perspectives
- Determine the appropriate time frame for the course of action
- Participate in appropriate information sharing organizations and,
- Periodically evaluate the firm's information sharing partners

Practical Cybersecurity Guidance

- **Governance and Risk Management**
- **Cybersecurity Risk Assessment**
- **Technical Controls**
- **Incidence Response Planning**
- **Vendor Management**
- **Staff Training**
- **Cyber Intelligence and Information Sharing**
- **Cyber Insurance**

Practical Cybersecurity Guidance

➤ Cyber Insurance

- Evaluate cyber insurance market
- Conduct periodic analysis of coverage adequacy
 - Legal Review
 - Fidelity Bond Reviews
- Evaluate alignment with Firm's Risk Matrix

Practical Cybersecurity Guidance

Summary of Critical Elements of Successful Cybersecurity Program

- **Governance and Risk Management**
- **Cybersecurity Risk Assessment**
- **Technical Controls**
- **Incidence Response Planning**
- **Vendor Management**
- **Staff Training**
- **Cyber Intelligence and Information Sharing**
- **Cyber Insurance**

Taming the Cybersecurity Lion

Key Takeaways

- **Top Priority for Regulatory Authorities**
- **Plentiful Resources to Stay Abreast**
- **Senior Management Ownership**
- **Understand Cybersecurity Threats**
- **Be Aware of Legal Implications**
- **Understand the Costs of a Cyber Attack**
- **Evaluate ALL of the Risks to your Firm**
- **Develop Robust, Risk-Based Cybersecurity Program**



Questions?



Resources & Handouts

- Introductions
- FINRA, Report of Cybersecurity Practices (February 2015) (“Sweep Report”)
- SEC NEP Risk Alert, Cybersecurity Examination Sweep Summary (February 3, 2015)
- Cybersecurity Guidance SEC Division of investment Management, April 2015
- SEC NEP Risk Alert, OCIE’s 2015 Cybersecurity Examination Initiative Vol. IV Issue 8 (Sept 15, 2015)
- In the Matter of R. T. Jones Capital Equity Management, Inc. (SEC) September 22, 2015
- A Framework for Cybersecurity, Supervisory Insights – FDIC, Vol. 12, Issue 2, Winter 2015
- SEC 2016 Exam Priorities January 11, 2016
- SIFMA Commends New Cybersecurity Action Plan from the Obama Administration, SIFMA, February 9, 2016
- Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015, The Department of Homeland Security, The Department of Justice, February 16, 2016
- NASAA, Compilation of Results of a Pilot Survey of Cybersecurity Practices of Small and Mid-Sized Investment Adviser Firms (September 2014)
- SIFMA, Small Firms Cybersecurity Guidance: How Small Firms Can Better Protect Their Businesses (July 2014),
- NCSL, Security Breach Notification Laws by State
- 2014 Cost of Data Breach Study: Global Analysis, The Ponemon Institute, Sponsored by IBM (May 2014)