OCIE Technology Controls Program

Cybersecurity Update

Chris Hetner
Cybersecurity Lead, OCIE/TCP
212-336-5546

Agenda

- Introduction (Role, Disclaimer, Background and Speech Topics)
- SEC Cybersecurity Program Overview
- Threat Actors
- Attacks that Impact the Markets
- Cybersecurity Industry Trends
- Exam Insights
- Industry Considerations and Best Practices

Introduction (Role, Disclaimer, Background and Topics)

- Chris Hetner with the SEC– the Cybersecurity Lead of the Technology Controls Program in OCIE
- *The Securities and Exchange Commission, as a matter of policy, disclaims responsibility for any private publication or statement by any of its employees. The views expressed herein are those of the author and do not necessarily reflect the views of the Commission or of the author' s colleagues upon the staff of the Commission."*
- 20 years cybersecurity experience building and leading global program @ EY (Practice Lead), GE Capital (CISO), and Citi (Programs and Ops)
- Topics to be covered
  - ✓Cybersecurity program overview
  - ✓Summary of key attacks, risks and trends impacting the market
  - ✓Best practices to minimize risk of cybersecurity

SEC Cybersecurity Program Overview

- Vision for the cybersecurity program is to shift the threat actors' attention and efforts away from the securities market by making the securities market an uninviting and hardened-security target.

- The goal is to establish a cybersecurity framework across the market, inform policy within the SEC and achieve a level of consistency by driving education, awareness and outreach.

- Newly created cybersecurity lead role is focused on providing leadership and support for cybersecurity matters across the national examination program within the SEC, particularly in the Technology Controls Program.

Threat Actors

Threat Actors	Attributes
Nation States	National governments seek to sabotage deals Protect and enhance the interest of local companies and industry Prevalent in deals involving assets or industries to be of strategic importance.
Organized Crime	See cyber-crime as a low risk/high return activity Profit driven entities Crime-as-a-Service emerging as a capability
Hacktivism	Politically motivated attacks Represent one of the most influential and powerful in cyberspace Launch attacks in retaliation to perceived injustices
Insider Threat	Insiders with trusted and privileged access Act with a lack of care whose errors increase compromise Applies to contractors and employees

Attack methods are similar.
Motivation, Sophistication and Impact vary.

Common Attacks that Impact the Market

Attack Method	Impact of Attack
Social Engineering	Social engineering attacks on wealth advisers and brokers in which the client is spoofed and the adviser/broker is tricked into sending funds belong to the client.
Ransomware	Crypto Locker which is a form a ransomware that encrypts files and programs across a suite of computers. Therefore disabling trade operations.
Stock Market Manipulation	Stock market manipulation is a growth area for criminals who hack into companies looking for information (new products or merger plans) that could affect a company's stock price, and then use this information to profit from trading.
Destructive Malware	Destructive Malware such as Wiper and Shamoon can permanently destroy data (books and records) that supports a Broker Dealer. Therefore severely impacting a firm's ability to continue operating.

Cybersecurity Industry Observations

Trend	Description
Specific Purpose Malware	• Customizes attacks for the purpose of stealing specific information or manipulating business processes • Common Targets- Investment Strategies, Intellectual Property, Account Numbers, SSNs, Executing Wire Transfers
Spear Phishing	• Email that appears to be legitimate customized to target high profile and individuals with privileged access to systems and data • Information about the target is garnered using various sourced (i.e. Facebook, LinkedIn, Associations)
Account Takeovers	• Exploit a Customer's Account and, In Many Instances, to Gain Seemingly Legitimate Access to Another Customer's Account.
Impact of an Attack	• Once firm experiences a cyber attack and suffers a loss it can take up to several months to remediate

In Many Cases Real Harm Does Not Come From the Cyber-attack Itself….Rather <u>It Comes from the Downstream Effect</u> of Having to Inform the Customers/Investors i.e.

The Reputational Damage is Potentially Irreversible and More So When Confidential Information/Data Now Resides Beyond the Control of the Organization!

Cybersecurity Exams: Salient Observations

- Firms were generally very responsive
- Vast majority of firms have implemented some form of information security policy
- 87%/majority of the examined firms reported that they have been the subject of a cyber-related incident
- Around half of the firms require an audit of vendors who have access to their network
- The designation of a CISO varied by firms' business model. Majority of BD firms designate a CISO while advisors direct their CTO to take on responsibility
- Over half of the firms received fraudulent emails, purportedly from customers, seeking to direct transfers of customer funds or securities

Industry Considerations

- I believe an important goal for the industry is to identify and prioritize cyber risk mitigation tactics.
- Cybersecurity must be engrained into the firms' culture.
- Cybersecurity is more than a technology risk; it is a business risk and it must permeate the enterprise risk management process.
- Industry must take it upon itself to make the right investments that address cybersecurity risk.

Cybersecurity Best Practices

Governance and Risk Management	• Risk Management Integration • Governance and Board/C level • Policy, Strategic Planning and Organization Management • Program Management and Workforce Planning
Operational Capabilities	• Identity, Access and Data Protection Controls • Cyber Intelligence and Incident Response • Cyber Threat Monitoring and Vulnerability Management • Third Party Risk Management
Business Integration	• IT Asset Management and Data Classification • Security Architecture • Legal and Compliance Management • Training and Awareness

Cybersecurity Initiative

Azam A. Riaz, CAIA, CRCP, CFE

June 18, 2015

DISCLAIMER

- *The Securities and Exchange Commission, as a matter of policy, disclaims responsibility for any private publication or statement by any of its employees. The views expressed herein are those of the author and do not necessarily reflect the views of the Commission or of the author's colleagues upon the staff of the Commission.*

OCIE CYBERSECURITY INITIATIVE

- 2014 Examination Priorities
- 2015 Examination Priorities

Purpose

- To assess cybersecurity preparedness in the securities industry and to obtain information about the industry's recent experiences with certain types of cyber threats

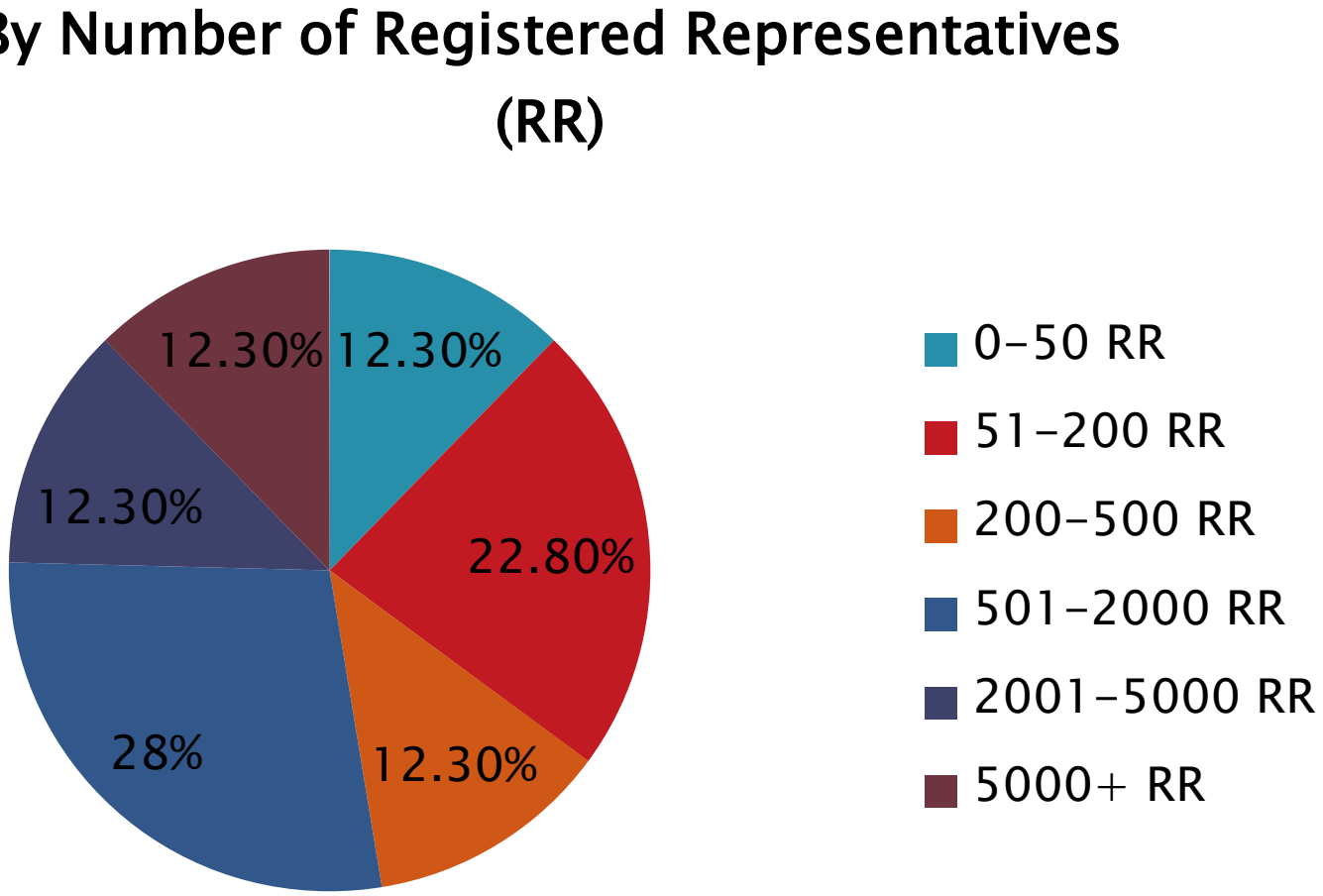
Focus Areas

- The entity's cybersecurity governance,
- Identification and assessment of cybersecurity risks,
- Protection of networks and information, risks associated with remote customer access and funds transfer requests,
- Risks associated with vendors and other third parties,
- Detection of unauthorized activity, and
- Experiences with certain cybersecurity threats.

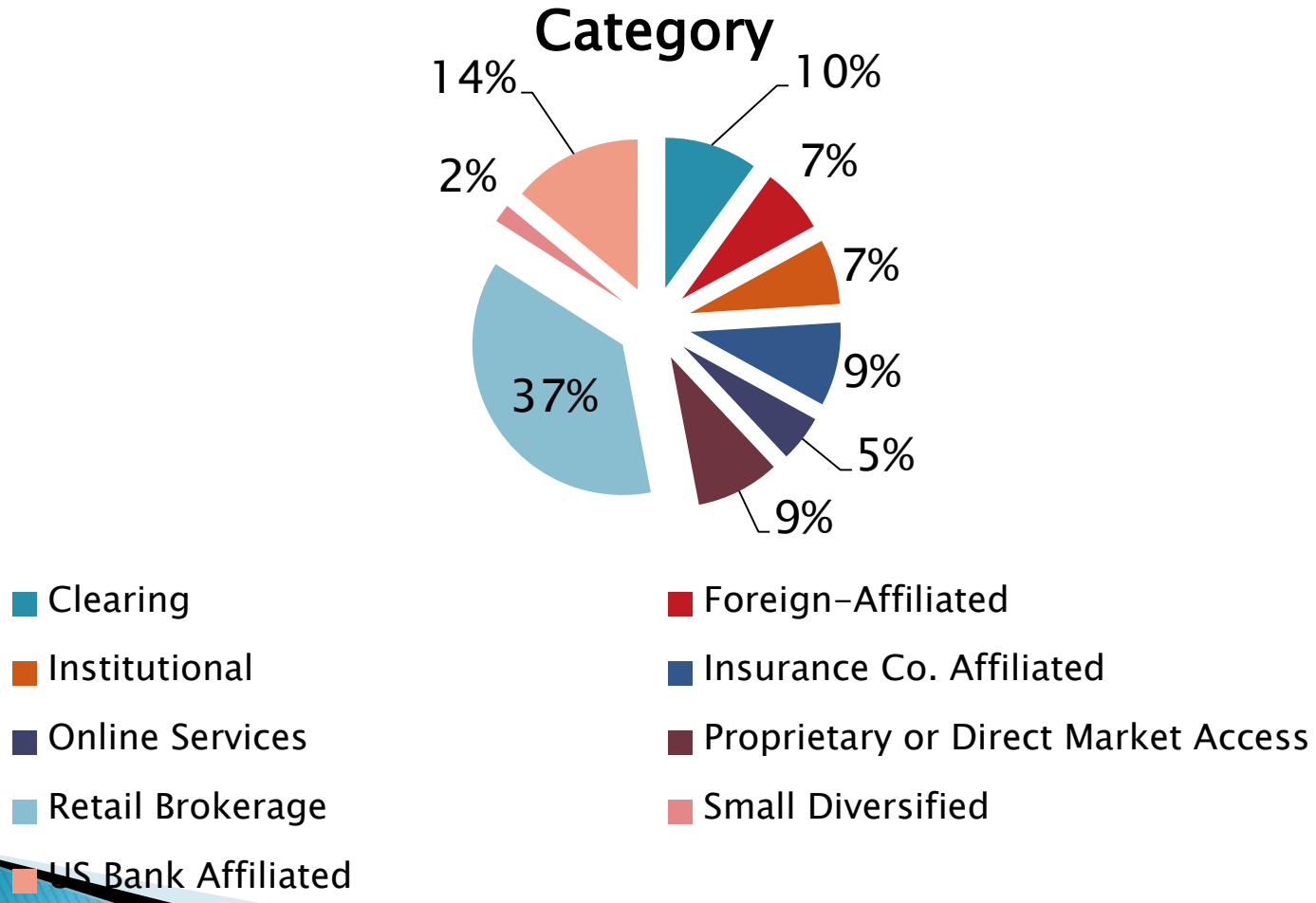
OCIE Cybersecurity Examinations

- 57 Broker-dealers
- 49 Investment Advisers

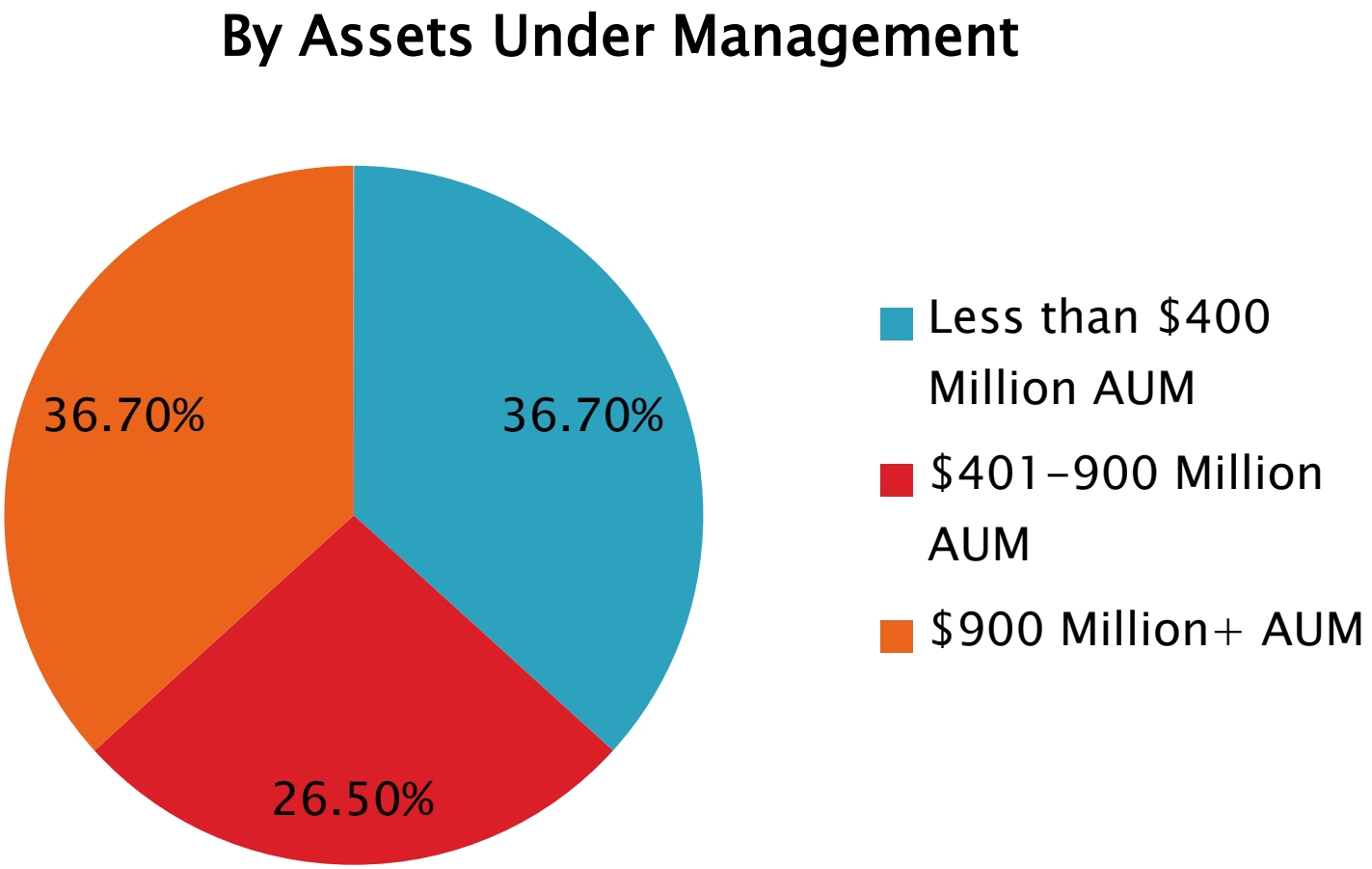
Breakdown of Examined BDs



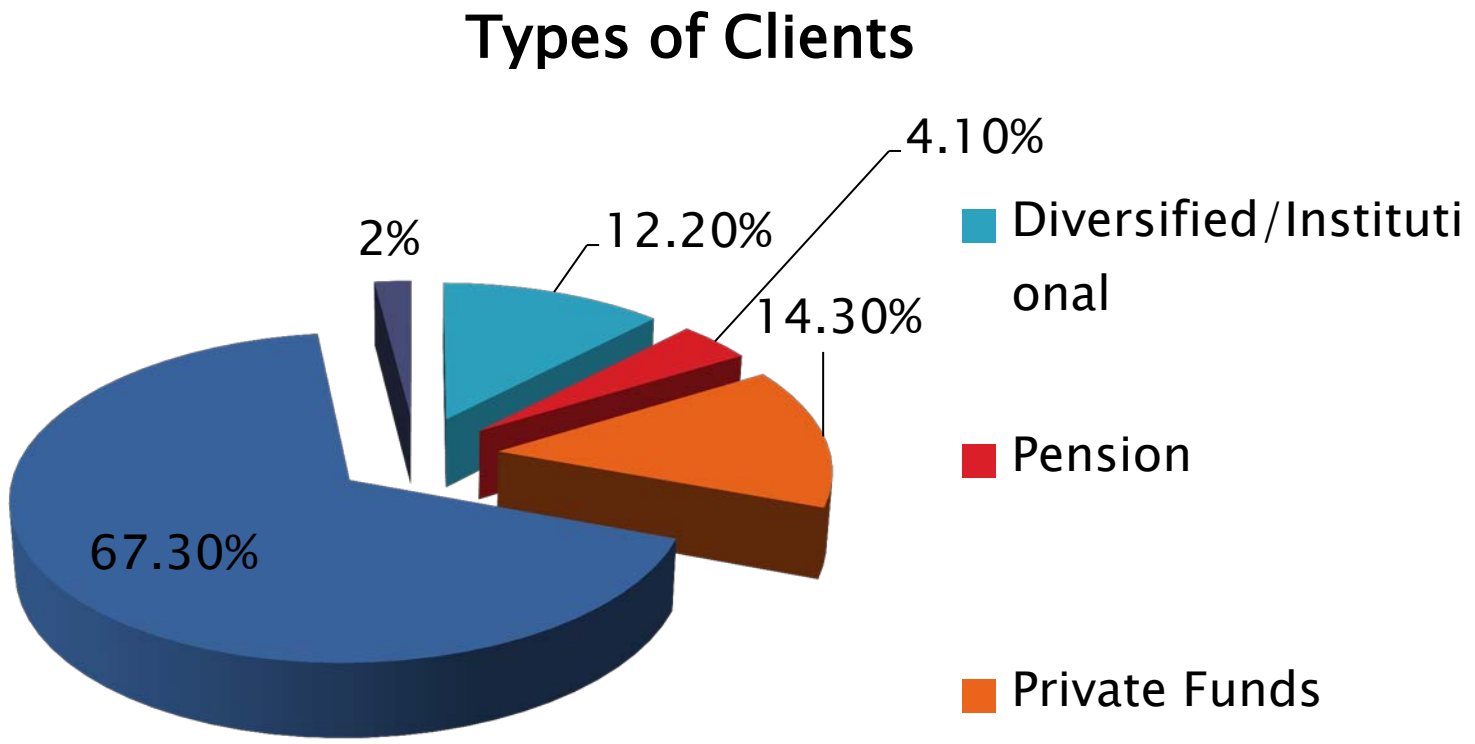
By Peer Group



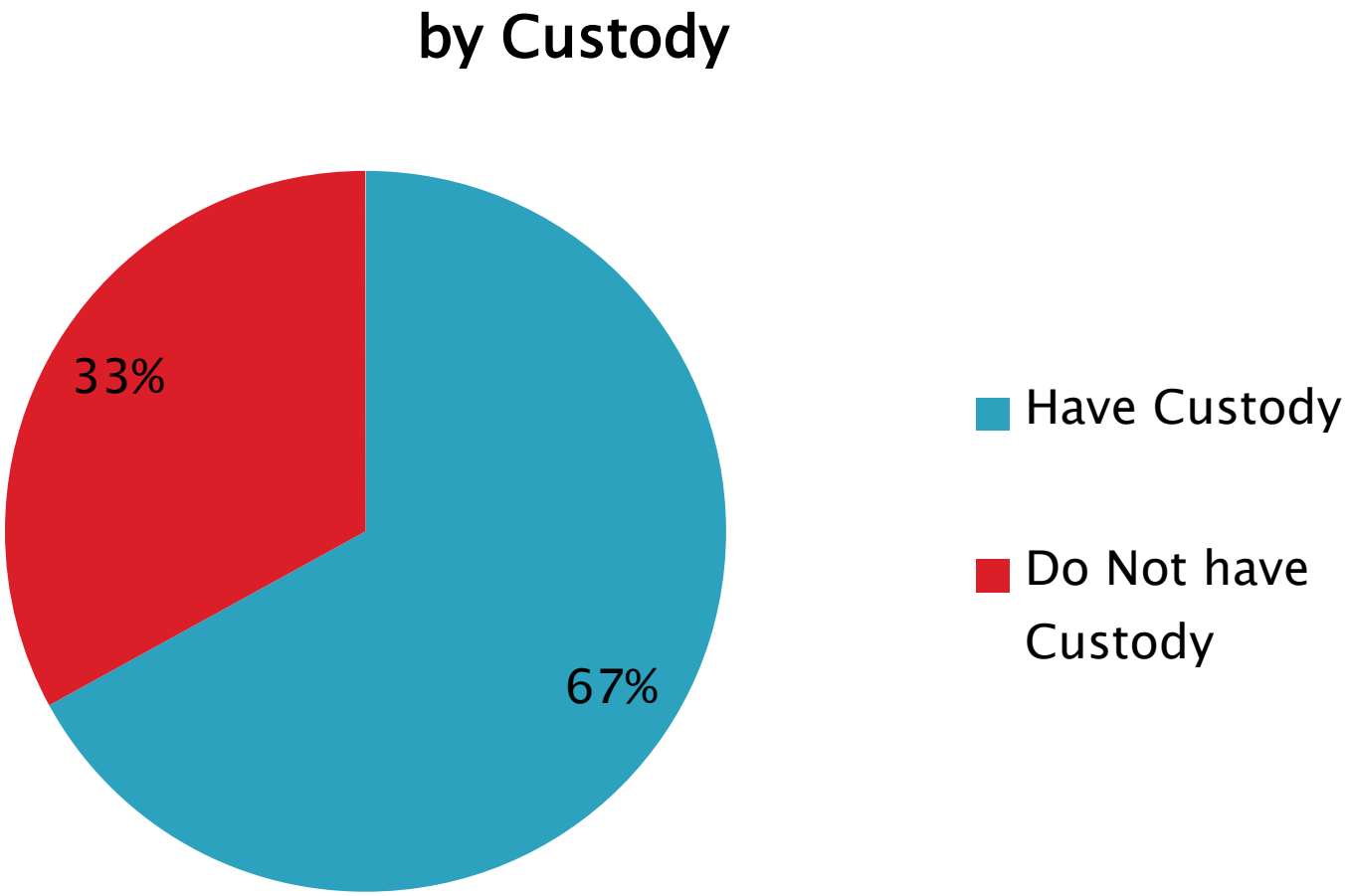
Breakdown of Examined IAs



Client Concentration



Custody of Client Assets



Key Personnel Interviews

- Business and operations;
- Detection and impact of cyber-attacks;
- Preparedness for cyber-attacks;
- Training and policies relevant to cybersecurity; and
- Protocol for reporting cyber breaches.

Summary exam observations

- CYBERSECURITY INITIATIVE

Written Policies and Procedures

Objective	Broker-Dealers	Investment Advisers
Adopted written information security policies	93%	83%
Policies address impact of cyber-attacks or intrusions	82%	51%
Policies address responsibility for client losses in cyber incidents	30%	13%
Security guarantees to protect clients against cyber-related losses	15%	9%
Use external standards and other resources to model information security architecture and processes	88%	53%

Periodic Risk Assessments

Objective	Broker-Dealers	Investment Advisers
Conduct periodic risk assessments on a firm wide basis to identify threats, vulnerabilities, and potential business consequences	93%	79%
Require cybersecurity risk assessments of vendors with access to firms' networks	84%	32%

Cyber-Related Incident

Objective	Broker-Dealer	Investment Adviser
Most examined firms reported being subject of a cyber-related incident	88%	74%
Received fraudulent emails related to transfer of client funds	54%	43%
Losses exceeding $5,000	26% due to fraudulent emails	1 adviser (See next row)
Losses exceeding $75,000	No broker-dealers had losses over $75,000	One adviser had losses exceeding $75,000
Employees did not follow identity authentication procedures	Yes for 25% of broker-dealers that had losses due to fraudulent emails	Yes for the one adviser that had losses exceeding $75,000
Reported to FinCEN	65%	1 adviser (aforementioned) reported to FinCEN
Reported to another Regulator or Law Enforcement	7%	Advisers generally did not report incidents to a regulator or law enforcement.

Information Sharing Networks

- Almost half of the broker-dealers (47%) were members of industry groups, associations, or organizations (both formal and informal) that exist for the purpose of sharing information regarding cybersecurity attacks and identifying effective controls to mitigate harm. Many of the broker-dealers identified the Financial Services Information Sharing and Analysis Center ("FS-ISAC") as adding significant value in this effort.
- While a few of the advisers also identified FS-ISAC as a resource, advisers more frequently relied on discussions with industry peers, attendance at conferences, and independent research to identify cybersecurity practices relevant to their business and learn about latest guidance from regulators, government agencies, and industry groups.

Mapping of Technology Resources

Objective	Broker-Dealers	Investment Advisers
Physical devices and systems	96%	92%
Software platforms and applications	91%	92%
Network resources, connections and data flows	97%	81%
Connections to firm networks from external resources	91%	74%
Hardware, data and software	93%	60%
Logging capabilities and practices	95%	68%

Risk policies related to vendors

Objective	Broker-Dealers	Investment Advisers
Incorporate requirements related to cybersecurity risk in contracts	72%	24%
Policies and Procedures related to security training for vendors and business partners authorized to access their networks	51%	13%

Other Matters

Objective	Broker-Dealers	Investment Advisers
Use of encryption	98%	91%
Provide clients steps that can be taken to reduce cybersecurity risks when conducting business with the firm on website or email	65%	75% of the 26% of advisers that primarily advise retail clients and permit those clients to access their account information online
Designation of Chief Information Security Officer (CISO)	68%	30% CISO; Mostly taken up by CTO, CCO, CEO, COO
Cybersecurity Insurance	58% (1 filed claim)	21% (1 filed claim)

Conclusions

- The staff is still reviewing the information to discern correlations between the examined firms' preparedness and controls and their size, complexity, or other characteristics.
- As noted in OCIE's 2015 priorities, OCIE will continue to focus on cybersecurity using risk-based examinations.

Advisers and the Identity Theft Red Flags Rule (Regulation S-ID)

- Registered advisers must comply with the Identity Theft Red Flags Rule.
- The final rule release states that even advisers who do not accept physical custody of their clients' accounts may be subject to the new rule if they can direct transfers or payments to third parties from a client's account or if they act as agents on behalf of individual clients.
- So if an adviser facilitates or directs bill payments for its clients or otherwise acts as their agent for financial purposes, the rule will likely apply.

Identity Theft Program

- Advisers falling within the rule must establish an identity theft program. The program must:

- Be in writing.
- Be approved by the board, an appropriate board committee, or senior management if the adviser has no board.
- Provide on-going oversight of the program by Board of Directors, an appropriate committee thereof or a designated senior management employee.
- Annual report suggested.
- Establish policies and procedures.
    - o To identify any identity theft red flags.
    - o To detect red flags.
    - o To respond to red flags in a way to prevent and mitigate identity theft.
    - o To update the program periodically to reflect changes in risk.

Identity Theft Program

- Guidelines in the appendix of the final rule include a number of examples of red flags, such as inconsistencies in personal identifying information, incomplete account opening information and changes in account usage.
- Provide training for employees.
- Provide oversight of service providers if the adviser has outsourced compliance. Adviser is ultimately responsible for compliance.
- Consider Guidelines for the program offered in appendix to the rule.

Settled Enforcement Case

- Adviser maintained signed Letters of Authorization ("LOA")
- One client's email account was hacked requesting wire transfers to a foreign account
- The third-party fraud was not discovered until three separate wires totaling $290,000 had been sent to the foreign bank.
- Adviser censured and fined a civil penalty of $250,000

Contact Information

Azam A. Riaz
Staff Accountant
US Securities & Exchange Commission
Brookfield Place,
200 Vesey Street, Suite 400
New York, NY 10281
(212) 336-0547
riaza@sec.gov

Questions?