# Welcome!

While we are preparing to begin, please:

- ❑ Download a pdf of the slides, if you'd like. See the Handouts panel.
- ❑ Use the Chat panel to tell the audience what the weather is like outside your window.
- ❑ Use the Chat panel to share something that you hope to gain out of this webinar.

SEC Compliance SOLUTIONS

*We've Got You Covered!*

# Practical Cybersecurity Compliance Guidance

## For SEC-Registered Advisers & Private Fund Managers

# Elizabeth Cope, CPA, CSCP, CIPM

## SEC Compliance Solutions LLC

I have been assisting investment advisers with compliance for over 15 years. I'm a firm believer that compliance does not have to be complicated. My motto is, "Keep it simple and practical!" Easy-to-manage policies and procedures are the best way to improve employees' understanding of compliance and have them buy-in to help avoid potential deficiencies.


- New Adviser Setup
  - Demystify the rules and regulations and keep compliance simple from the beginning
- Annual Compliance Review
  - Streamline policies and procedures and implement systems to manage and document an easy, organized, and methodical annual review
- Mock SEC Exam
  - Prepare personnel to be examined, identify gaps and potential issues relevant to the firm, provide practical solutions for how to remedy them, and assist with post-exam implementation

# Jason Elmer

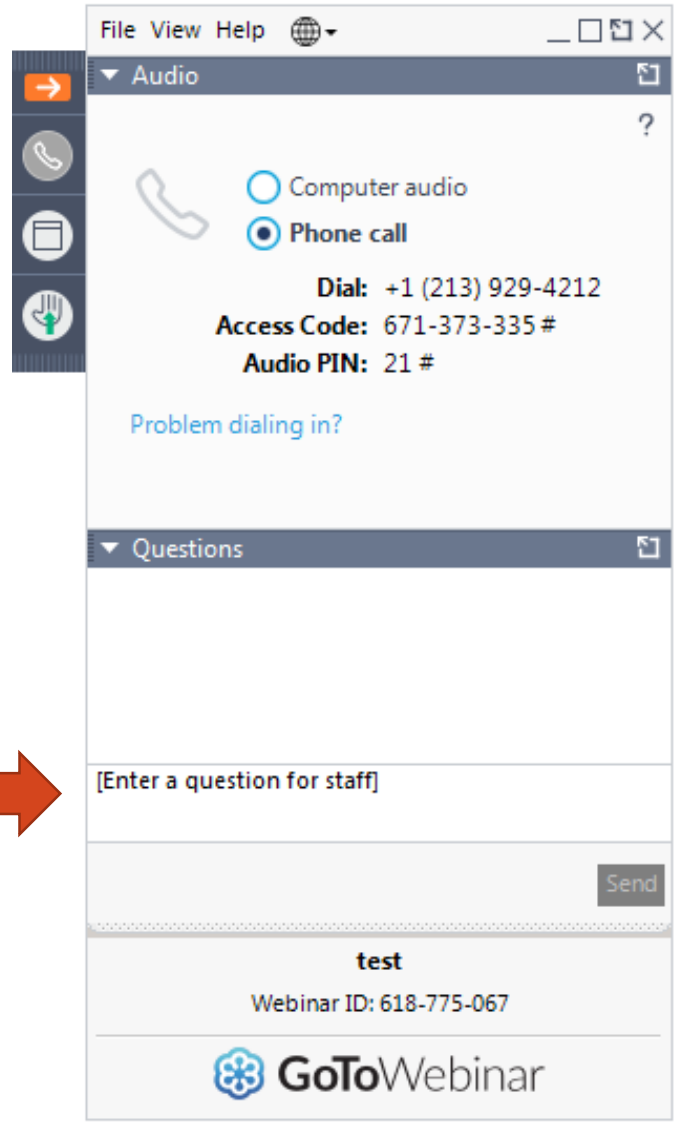
## Drawbridge Partners

Jason has more than 20 years of experience within the financial services space, specifically in providing FinTech solutions to the banking community, hedge funds, and private equity managers.

Jason has worked closely with a number of banks, hedge funds, and private equity managers across a variety of areas of their businesses, including establishing cybersecurity and operations infrastructures; completing risk assessments; selecting appropriate service providers; performing vendor due diligence reviews; and preparing for and dealing with regulatory examinations.


- Program Development
- Vendor Due Diligence
- Risk Assessment
- Vulnerability Management
- Penetration Testing
- Policies and Procedures
- Phishing and Training
- Data Privacy (GDPR)
- Business Continuity Planning
- Portfolio Company Reviews

# Ask Questions!




Type your questions here

To make it larger, pop it out of the panel here

# Today We'll Cover

- What the SEC expects of you regarding cybersecurity
- How to meet the SEC's expectations
  - Whether your cybersecurity policies are appropriate
  - The importance and components of an incident response plan
  - The most important considerations in reviewing third-party service providers that have access to sensitive information
- Areas where advisers commonly have gaps and deficiencies
- The types of testing available and what kind of cybersecurity testing my be the most appropriate for your firm
- What to expect if you hire someone to conduct testing

# Key Terms

# Key Terms

- Business Email Compromise (BEC)
- Phishing
- Vishing
- Malware
- Ransomware

# What the SEC Expects – 2019 Exam Priorities

# What does the SEC expect?

- Assess Your Cybersecurity Risks
  - Evaluate internal & external risks
  - Consider how and where sensitive information is stored
  - Review controls and processes in place
- Have a Cybersecurity Plan to Mitigate Your Risks
- Some Form of Testing
  - Vulnerability, Penetration, Phishing tests

# What does the SEC expect? Cont.

- Policies and procedures
  - Written Information Security Policy
  - Incident Response Plan
- Vendor Due Diligence
  - Review the risk posture of your critical third parties
- Educate Your Personnel
  - Communicate common threats
  - Create a culture of security and train your employees
  - Remind everyone of the policies in place to prevent threats

# What does the SEC expect? Cont.

- Data Classification & Access Controls
- Data Loss Prevention

# Enforcement Actions

- Cybersecurity Enforcement Actions
- In 2016, Morgan Stanley paid $1 million in fines for failure to protect client information
  - An Employee transferred 730,000 client records onto his personal computer which was hacked into by third parties
- In 2016, RT Jones paid $75,000 for failing to adopt policies and procedures for safeguarding
  - Data stored on third-party web server, which was hacked. The firm appropriately responded to the attack and, to date, no one was harmed
- In 2018, Voya paid $1 million in fines for failure to adopt policies and procedures for protecting client information
  - Technical support provided username and passwords to impersonators who used the data to access nonpublic client records

# How to meet the SEC's expectations

# Assess Risk

- The First Step!
- Assess both internal/external threats to your systems and people
  - Access – are passwords strong, do you have MFA, Group/Role based access.
  - People – are they educated on the threats?
- Once the risks are identified, implement steps to mitigate
- Document your risk assessment to provide to SEC if requested

# Develop a policy

- Tailor it to your Firm, do not have a boiler plate procedure
- Make sure you understand it
- Review regularly to make sure:
  - Consistent with actual practice
  - Reasonably designed
- Be able to provide SEC copy of plan and any reviews of the plan

# Addressing a breach

- If you had a breach, take care of it immediately
- Document!!
  - The date occurrence was identified
  - How it occurred
  - What you do to remedy the situation
  - Any communications made to clients, FBI, etc.
  - Remedial steps taken to prevent reoccurrence
- Cybersecurity Insurance – if you have a breach they cover the costs of forensic testing/review, which can range from $30,000-$50,000.
- Provide SEC documentation if requested

# Third Party Service Providers

- If they have access to sensitive information
- Complete due diligence initially and ongoing on an annual basis
- Assess the controls they have in place to protect your Firm and clients

# Hot Button Questions

# Common question we get

- What do you think about moving into the cloud?  Does this increase our risk of exposure?
- Is having a complex password (i.e. capital letter, lowercase letter, symbol, 8 min. characters) still the acceptable method?  Or is the industry moving towards using long phrases?
- Do I need to have Cybersecurity insurance?

# Common Gaps & Deficiencies

# Policy vs Employee Practices

- Inadequate Policies
  - Not consistent with actual practice, procedural exceptions are created but not documented
  - Outdated
  - Do not address risks of the firm
- Lack of Training
  - Employees are not reminded of the threats
  - Employees do not understand their responsibilities pertaining to security
- Not Testing the Plan

# Types of Testing and How to Know What's Appropriate for Your Firm

# Vulnerability Scanning vs Penetration Testing

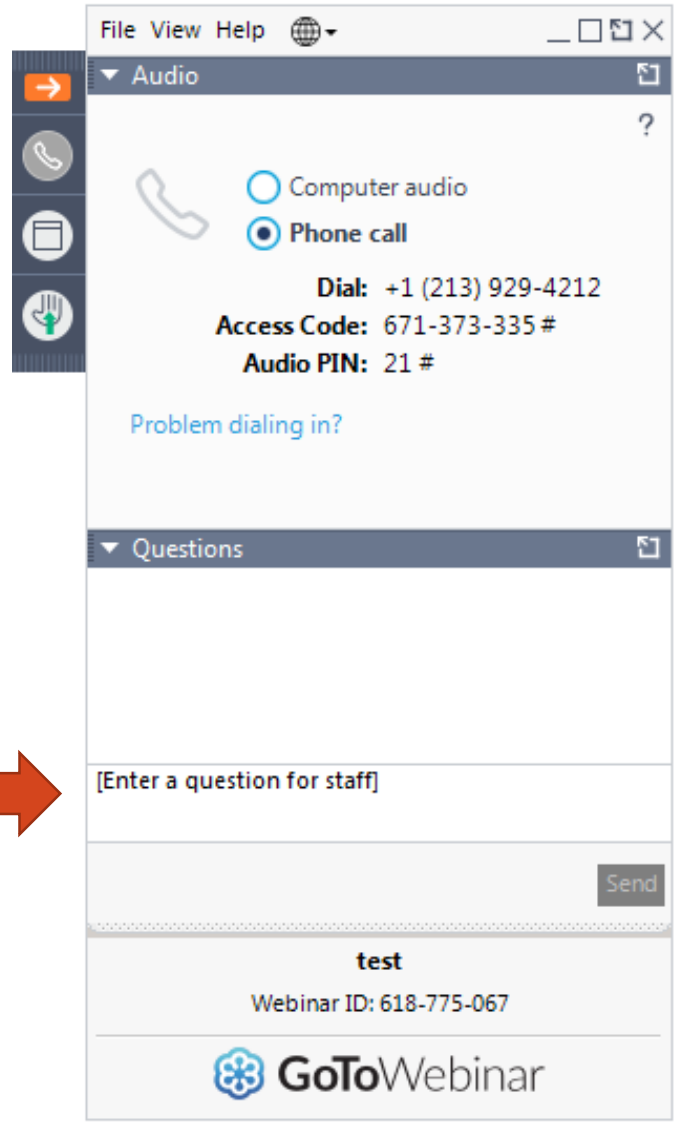
- What is a vulnerability scan?
- What is a penetration test?
- The right recipe

# What to expect if you hire someone to conduct testing

# Why hire a third party to conduct testing?

- A second set of eyes
- Unbiased report
- Prevents ‘auditor, auditing themselves’ scenario
- Industry expertise

# Questions?




Type your questions here

To make it larger, pop it out of the panel here

# Additional Compliance Training

- Subscribe to Our Mailing list
  - Regulatory Updates
  - Deadline Reminders
  - Educational Articles & Whitepapers
  - Educational Webinars & Events
  - https://seccsllc.com/email-opt-in-consent/
- Visit Our Blog
  - https://seccsllc.com/compliance-blog/

# Thank you for joining us!


Elizabeth Cope, CPA, CSCP, CIPM
Managing Member
SEC Compliance Solutions LLC ›

liz@seccsllc.com
(541) 227-2336



Jason Elmer
Managing Partner
Drawbridge Partners ›

jason.elmer@drawbridgepartnersllc.com
(917) 660-1975