

# OCIE Cybersecurity Risk Alert: Leaving your lifeboat at shore...

September 8, 2017

We have a lifeboat—but (oops!) it's back at shore.

When it comes to lifeboats—and cyber-security policies—you don't want to have an “oh shoot” moment.

Have you seen the recent announcements from the SEC's OCIE Cybersecurity Risk Alert? It summarized observations from the OCIE's second cybersecurity survey of financial services firms in relation to cybersecurity-related policies and vulnerability to attack. Many firms were doing some things right...but overall, there's major room for improvement.

## **The good news included:**

- Nearly all broker-dealers and almost half of the advisers and funds conducted penetration tests and vulnerability scans.
- All surveyed firms utilized some data loss prevention tool.
- Most firms specifically identified employees to be in charge of cyber-related responsibilities and had cybersecurity organizational charts.
- Almost all firms conducted vendor risk assessments.

## **Here's the not-so-good news:**

Most of the firms had information protection policies that were too narrow, too vague or not properly enforced or maintained. A policy that doesn't fit your firm may sound like it fits the bill, but when push comes to shove, it's useless.

## **Best practices: What should your RIA do?**

The OCIE encouraged all firms to:

- Create detailed cybersecurity-related instructions that implement policies; for such things as penetration tests, security monitoring and system auditing, access rights, and reporting exposed sensitive information.
- Maintain prescriptive schedules and processes for testing data integrity and vulnerabilities, including vulnerability scans and patch management policies.
- Establish and enforced controls to access data and systems. For instance, “acceptable use” policies, required and enforced restrictions and controls for mobile devices, third-party vendor management, and employee termination protocol.
- Mandatory employee training.
- Engage senior management.

- Maintain an inventory of data, information, and vendors.

Be honest with yourself...

Does your firm have policies somewhere on a shelf?

Are these policies actually specific to your RIA and the way you operate?

Are you actually implementing these policies?

If all of this feels like uncharted waters—let us help you navigate.