The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 36004

January 30, 2025

ICI Cyber Incident Tabletop Exercise 2024 After-Action Report

[36004]January 30, 2025TO:ICI Members
Chief Compliance Officer Committee
Chief Information Security Officer Committee
Chief Risk Officer Committee
Global Information Security Officer Committee - London
Global Information Security Officer Committee - Tokyo
Operational Resiliency Committee
Operations Committee
Securities Operations Advisory Committee
Technology Committee
Transfer Agent Advisory CommitteeSUBJECTS:Compliance
Cybersecurity
International/Global
Operations
Recordkeeping
Risk Oversight
Technology & Business Continuity
Transfer AgencyRE:ICI Cyber Incident Tabletop Exercise 2024 After-Action Report

ICI is pleased to share its After-Action Report (AAR) for the July 2024 Cyber Incident Tabletop Exercise. The report recaps the Tabletop Exercise and provides key findings and takeaways for ICI and its members as we collectively optimize operational resiliency for the asset management industry—to the benefit of individual investors.

ICI Cyber Industry Tabletop Exercise

ICI organized and facilitated an in-person industry tabletop exercise (exercise) on July 24, 2024, hosted by ICI member AllianceBernstein in New York, NY. Simulating a ransomware attack on a single ICI firm, the exercise asked participants to assume the impacted firm was their own, and that all financial markets, counterparties, and service providers were otherwise operating normally. The exercise, covering a three-day period, provided participants a forum for collaboration and information sharing under simulated stressed conditions, raised awareness of ransomware considerations, and allowed participants to practice and enhance their crisis management and cyber incident response plans and recovery strategies. Participants had business backgrounds in business continuity, information security, technology, risk and compliance, and industry operations.

After-Action Report

The AAR summarizes participant insights on internal and external response challenges and related remediation strategies. In addition, the AAR highlights lessons learned and key takeaways, all which stress expanding operational resiliency through robust planning, technology deployment, and ongoing testing of capabilities. Participants particularly cited the need for robust liquidity and cash management preparations from a functional and reputational perspective. The AAR ends with a checklist, distilled from tabletop participant insights and observations, on how to effectively prepare for and execute a crisis management and cyber mitigation strategy in the face of a significant business disruption, such as a ransomware attack.

The report is publicly accessible by clicking the link above or by accessing the "ICI White Paper" section of the ICI website (ici.org/publications).

ICI is committed to supporting its members through this and future exercises that span functional roles and that seek to optimize operational resiliency of the asset management industry. Please contact the undersigned (peter.poulos@ici.org; 202-326-8302) or Andrew Kayiira, Director, Technology and Financial Innovation (andrew.kayiira@ici.org; 202-326-5928) with questions.

Peter Poulos
Senior Director, Information Security
