

ICI OPERATIONS

JANUARY 2025

ICI Cyber Industry Tabletop Exercise 2024 AFTER-ACTION REPORT

Contents

1 Overview

2 Scenario and Methodology

3 Summary of Breakout Session Discussions

4 Lessons Learned and Key Takeaways for ICI Members

5 Key Takeaways for ICI

5 Conclusion

6 Appendix A: Checklist of Resiliency Considerations

9 Appendix B: List of Participating Organizations

“Through our Cyber Industry Tabletop Exercise, ICI members had the invaluable opportunity to evaluate their response and recovery capabilities and explore the best strategies to fortify them. Cybersecurity is a responsibility of every person and firm in our industry, and ICI is dedicated to doing whatever we can to work with our members and strengthen our collective resilience to evolving cyber threats.”

Eric Pan, President and CEO, Investment Company Institute

The content contained in this document is proprietary property of ICI and should not be reproduced or disseminated without ICI's prior consent. It is not intended to be, and should not be construed as, legal or investment advice. Each firm should make independent decisions, if any, based on the information in this document and other appropriate considerations.

Copyright © 2025 by the Investment Company Institute. All rights reserved.

ICI Cyber Industry Tabletop Exercise 2024

AFTER-ACTION REPORT

Overview

The asset management industry faces an escalating battle against cybercriminals employing increasingly sophisticated tactics. From state-sponsored attacks to ransomware-as-a-service (RaaS) platforms enabling low-skilled criminal infiltrations, the threat landscape is more complex than ever. Unlike cyber-attacks that focus on service disruption of a common industry service provider or infrastructure without necessarily seeking direct financial gain, ransomware attacks are more isolated in scope and are focused on extorting victims. Ransomware attacks are increasing and create significant commercial and reputational risks for the affected organization, often requiring substantial time and resources to mitigate. These attacks can also have spill-over reputational and operational impacts on related industry organizations.

To address the common risk of a ransomware cyber-attack, the Investment Company Institute (ICI) hosted an in-person industry tabletop exercise on July 24, 2024, at AllianceBernstein in New York, NY. Thirty-three (33) ICI member firms and over fifty (50) attendees, including facilitators and observers, participated in the exercise, which was planned and facilitated by ICI and volunteers from its Chief Information Security Officer (CISO) and Business Continuity Planning (BCP) committees.*

The objectives of the tabletop exercise were as follows:

1. to provide a forum for collaboration and information sharing under simulated stressed conditions,
2. to raise participant awareness of ransomware considerations, and
3. to allow participant firms to practice and enhance their crisis management and cyber incident response plans and recovery strategies.

Simulating a ransomware attack on a single ICI firm over a three-day period, participants were asked to assume the impacted firm was their own, and that all financial markets, counterparties, and service providers were otherwise operating normally. From this perspective, participants assessed and responded to common questions within small group assignments and with the broader group about response plans and recovery strategies while considering various business, client, risk, compliance, and technology considerations.

* Committee members from AllianceBernstein; Artisan Partners; Capital Group; Lord, Abbett & Co.; and Saturna Capital formed the planning team and served as co-facilitators of the tabletop exercise. A list of all participating firms is provided in Appendix B.

Scenario and Methodology

The tabletop exercise followed a scenario whereby a fictitious cyber-criminal organization “Lockbit X” successfully stole administrative credentials to assume control of the hypothetical ICI firm’s corporate network.

ICI organized exercise participants into groups of 6–8 participants led by a facilitator. These groups reflected both the diversity of participating firm size and participants’ business and technical expertise. Groups responded to questions at three distinct points in the timeline of the exercise, reporting responses to the broader group as the exercise progressed.

Introduction

At 11:15 AM ET on a Thursday, the IT service desk received reports of workstation and connectivity issues from Fund Operations employees. Initially assumed to be a common technology infrastructure issue, the situation escalated rapidly.

By 11:45 AM ET, the outages had spread to a large part of the firm, and employees were locked out of their workstations. A ransomware message appeared on their screens, demanding \$35 million in Bitcoin within 24 hours, or \$70 million if the deadline was missed.



INJECTION 1: Day 1 (First 2 Hours)

- » **Internal Events:** All employees, including cybersecurity and technology teams, are locked out of the company network. Corporate communications systems are unavailable. The cyber incident response team is mobilized to investigate.
- » **External Events:** Industry counterparties notice the firm has gone offline. Clients are unable to access their financial statements or reach their financial advisors online. News of the firm’s outage begins spreading across social media.

Breakout Session: Cyber Incident Response and Crisis Management Team Focus

- » Do you have a Ransomware Response and Recovery Plan?
- » Are there ways for you to break back into your “locked” network?
- » Has an externally hosted firmwide emergency management communications system been established?
- » Who is communicating with the media, clients, counterparties, service providers, and regulators?

INJECTION 2: Day 1 (3 to 8 Hours)

- » **Internal Events:** Employees still locked out, communication systems down, response team investigating.
- » **External Events:** Counterparties and clients notice the outage, news spreads on social media.

Breakout Session: Business and Client Response Team Focus

- » What essential and time-sensitive obligations does your firm have today? For example:
 - » Processing client purchase and redemption orders
 - » Executing and settling in-flight trades
 - » Ensuring fair pricing on all transactions/striking NAV
 - » Reporting trade confirmations and account statements
 - » Manage liquidity needs, including cash flows (e.g., scheduled payments and redemption requests)
- » What are your top priorities at this point?
- » How will you fulfill your intraday client obligations and meet liquidity needs?
- » How can your custodian bank help?
- » Who else do you call for help?
- » Are you considering paying the ransom?

INJECTION 3: Day 2 to Day 3+

Situational Update (Day 2): Corporate network remains locked. Outage estimated to extend into the weekend and possibly into next week. Crisis Management Team and external legal counsel advise not to pay the ransom. Alternate means of external communication are being used. Clients remain concerned. Cash reserves and credit lines are stressed to meet increased cash flow demands.

Breakout Session: Business and Client Considerations

- » What help are you able to get from your custodian or other providers?
- » What are your priorities now? How are you addressing them?
- » What can you do to fulfill your client obligations and meet liquidity needs from yesterday and today? What about over the weekend and into next week?

Breakout Session: Technology Considerations

- » How are your technology service providers able to help with recovery?
- » Would your current recovery and restoration capabilities work in this scenario? If yes, how long do you estimate it would take?
- » Do you have data vaulting capabilities to securely backup mission critical systems and data in an isolated “air-gapped” emergency environment?

Summary of Breakout Session Discussions

In addition to discussion during the tabletop exercise, each group provided ICI with notes summarizing their insights, observations, and conclusions from each scenario injection. ICI summarized participant responses, grouping information by internal versus external focus.

INTERNAL

Response Challenges and Capabilities

Network/System Lockout: The complete lockout of employees from the company network, including cybersecurity and technology teams, severely hindered internal communication. Traditional corporate communication systems, such as email, chat, and IT service desks, were unavailable, forcing teams to rely on alternative methods.

Coordination Difficulties: Without access to the primary communication systems, coordinating the response efforts became challenging. Teams had to quickly adapt to using off-channel communication tools to assemble the Cyber Incident Response Team and manage the crisis.

Impact Assessment and Third-Party Service Provider Support: Playbooks, mobile network device access, and other means were used to assess the impact of the lockout, along with engaging third-party service providers to assist in response and recovery.

Ransomware Response Plans: Most participants had plans in place, including the use of off-network communication tools and “break glass” (i.e., critical emergency) accounts for network access.

Data Vaulting and Recovery Capabilities: Ensuring data vaulting capabilities and restoring Active Directory to a clean state were critical. In addition to the use of “break glass” accounts, firms also considered using alternate Microsoft tenants for emergency access. Participants also emphasized the importance of having immutable backups in isolated environments and regularly testing recovery capabilities.

EXTERNAL

Response Challenges and Capabilities

Client Communications: With client portals impacted, self-servicing capabilities declined and placed additional burden on call centers. Clients were unable to access their financial information or reach their financial advisors online, leading to increased anxiety and concern. With voice-over-IP phones prevalent in call centers, firms with internally managed call centers had to find alternative ways to communicate with clients, such as using mobile phones. Firms with call centers managed by a third-party provider were able to leverage them to communicate with clients.

Client Obligations: Ensuring updated records, managing liquidity, and fulfilling intraday obligations were top priorities. Participant firms used alternate means (such as compliance hotlines) for manual trades and instructions.

Media Communications: News of the firm’s outage spread rapidly on social media, putting additional pressure on the firm to manage its public image and provide timely updates. Designating points of contact for media and ensuring consistent messaging on multiple platforms were critical to maintaining trust. Transparent communication with clients and stakeholders was emphasized to minimize panic. Firms considered using CEO TV interviews and regular social media updates to reassure clients.

Regulator and Law Enforcement Communications: Reporting the incident to regulators (e.g., SEC) and law enforcement (e.g., FBI) required careful coordination and clear communication. Firms had to ensure that all necessary information was conveyed accurately and promptly, despite the communication challenges. Incidents were reported to regulators and the FBI with considerations for ransom payment decisions. Firms engaged external counsel and law enforcement as needed.

Lessons Learned and Key Takeaways for ICI Members

Based on group discussion notes, breakout session discussions, and broader group discussions following each of the injections, the following lessons learned and key takeaways were identified:

- » **Alternative Communication Methods:** The exercise highlighted the importance of having robust alternative communication methods in place. Firms should ensure they have access to off-network communication tools and pre-defined communication protocols for crisis situations.
- » **Clear Roles and Responsibilities:** Establishing clear roles and responsibilities for communication during a crisis is essential. Firms should designate specific individuals or teams to handle internal and external communications, ensuring a coordinated and effective response. Ensure top-down and bottom-up responsibility across the organization. Much of this is accomplished by creating thorough crisis management–related documentation and procedures that are routinely reviewed and updated as the organization evolves.
- » **Regular Testing and Training:** Regularly testing an organization’s communication plans and training its staff on alternative communication methods can optimize preparedness. Conducting internal tabletop exercises and simulations can provide valuable insights into potential communication challenges and areas for improvement and remediation. Educate business leaders and staff on their roles in disruptive events. Also, consider the emotional responses of people during a crisis and incorporate support resources in crisis management plans.
- » **Dedicated Ransomware Recovery Environment:** The Dedicated Ransomware Recovery Environment is an isolated environment from the main production network to prevent the spread of malware and ensure a secure space for restoring data and systems. It requires dedicated infrastructure with specific systems and resources allocated solely for recovery purposes. By dedicating such an environment, organizations can more effectively and quickly recover from ransomware attacks, minimizing downtime and financial loss. Members must evaluate the cost of such an environment versus the risk of not being covered.
- » **Plan to Manage Liquidity:** Based on fund prospectuses, members may have some leeway in paying redemption proceeds. While there are significant reputational risks in delaying payment of redemption proceeds, such a strategy could be pursued in conjunction with lines of credit and other liquidity management strategies to manage through liquidity challenges. During the tabletop exercise, this area was cited by participants as one of the most critical concerns to manage and mitigate. A well-thought-out strategy to manage liquidity before the fact will help funds maintain optimal liquidity under the circumstances.



Key Takeaways for ICI

The exercise and subsequent discussions with participants also yielded takeaways for ICI.

- » Host annual tabletop exercises to engage members across legal, risk, compliance, technology, and operations functions and simulate additional scenarios.
- » Provide a forum to exchange ideas and develop practices on business and technical recovery solutions tailored to the asset management industry. Participation of ICI members who are also custodians/asset servicers is essential to the success of this effort.
- » Partner with ICI members and other industry organizations to update existing and develop new industry incident response mechanisms and communication protocols in the financial sector.

ICI is committed to supporting its members in this way to the betterment of individual investors and will investigate future action.

Conclusion

The ICI Cyber Industry Tabletop Exercise successfully highlighted the importance of preparation, communication, collaboration, and continuous improvement in managing cyber incidents and ensuring business resiliency. Participants in general deemed the exercise as beneficial and informative, with participants appreciating the opportunity for knowledge sharing and networking. The insights gained from this exercise will help strengthen the industry's resilience and readiness to effectively respond to future disruptions.



Appendix A: Checklist of Resiliency Considerations

The following checklists consolidate ICI member 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. Members should use this as one resource to help guide their development of sound business and cyber resiliency practices:

Crisis Management and Cyber Incident Response Considerations

Planning and Preparation

1. Establish and maintain documented crisis management and cyber incident response plans.
2. Keep response and communication plans off-network (digital and/or paper-based).

Communication Strategies

3. Involve corporate communications and/or investor relations in planning; engage a public relations (PR) firm if necessary.
4. Prepare pre-scripted communications for internal and external stakeholders, including public statements and press releases for media.
5. Ensure crisis management and cyber incident response teams are aligned with key internal (e.g., corporate communications) and third parties (e.g., PR consultant) to develop consistent and complimentary communications.

Roles and Responsibilities

6. Establish and maintain crisis management and cyber incident teams.
7. Define roles and appoint a crisis leader and incident manager along with their delegates for effective decision-making and facilitation.
8. Clarify roles and responsibilities of external counsel, insurance providers, and critical third-party service providers.

Detection and Reporting

9. Engage threat intelligence, negotiation partners and law enforcement contacts ahead of time.
10. Update and implement clear escalation protocols and communication scripts for cyber incident reporting for internal staff, clients, third-parties, regulators, and law enforcement.

Regular Testing and Exercises

11. Conduct regular testing and exercises with internal stakeholders to build muscle memory.
 12. Develop and test plans with multiple scenarios and involve external cyber counsel, law enforcement, third-party providers, and other stakeholders in your exercises.
-

Business Considerations

Business Considerations

13. Identify time-sensitive business decisions needed within the initial 24–48 hours.
14. Understand critical process workarounds or contingency methods for affected systems. Ensure workarounds are routinely evaluated and tested for readiness.
15. Determine how key in-house functions (e.g., portfolio and investment management, client servicing, distribution) are affected by the incident and how those solutions may be supported (e.g., third-party, recovery site).
16. Partner with key service providers to plan for various scenarios and ensure appropriate notification procedures are in place in the event of a crisis. Consider joint tabletop exercises and tests to improve response and recovery.

Client Considerations

17. Managing investor and client expectations.
18. Align external messaging with corporate communications, crisis management, and other teams for consistency.
19. Maintaining a list of client contacts in the crisis management plan and ensuring clear communication channels are in place to mitigate investor panic and reinforce the safety of client data and holdings.

Risk Management Considerations

20. Develop a liquidity plan, including lines of credit, other sources of liquidity, and procedural measures are in place to prevent or minimize possible impact to investors and counterparties.
21. Prioritize critical funds, portfolios, and accounts in the event cash availability is curtailed.
22. Prepare for third-party pull back due to possible risk of contagion and/or implication due to the incident (this may transition concerns from a cyber to a legal event).

Compliance Considerations

23. Ensure communication channels with compliance teams are established and functional for critical operations to seek guidance during a crisis.
 24. Understand both domestic and global regulatory requirements, provide necessary notifications, and test these processes with third-party partners.
-

Technology Considerations

Off-Network Communication System

25. Assess off-network communication capabilities.
26. Establish and use an off-network emergency notification system for communication and coordinating response efforts.

Alternate Email and Productivity Solution

27. Establish an alternate tenant or instance of your primary email and productivity platform (e.g., Microsoft 365) as a “break glass” solution to ensure resumption of secure electronic communication and collaboration capabilities.

Data Vaulting with Air-Gapped Immutable Copies of Data

28. Assess off-network data recovery capabilities. Traditional disaster recovery systems may not be effective in ransomware scenarios.
29. Develop and maintain independent and secure network and data environments that can be accessed to maintain continuity of operations.
30. Implement data vaulting with immutable copies of data.
31. Ensure the backup environment is “air-gapped” (i.e., physically isolated from the internet or unsecured networks), and tested regularly within recovery point objectives is also essential to estimate time to decrypt and restore in a crisis.



Appendix B: List of Participating Organizations

AllianceBernstein L.P.	MFS Investment Management
Allspring Global	Mutual of America
Artisan Partners Limited Partnership	Neuberger Berman Investment Advisers LLC
Baron Capital	PIMCO
BNP Paribas	Resolute Investment Managers, Inc.
Brown Advisory LLC	Saturna Capital
Capital Group	Schwartz Investment Counsel, Inc
Charles Schwab Asset Management	Sheltered Harbor*
Cohen & Steers	SIFMA*
Diamond Hill Capital Management	T. Rowe Price
Dimensional Fund Advisors	Thornburg Investment Management
Domini Impact Investments LLC	Ultimus Fund Solutions
Guggenheim Investments	UMB Financial / UMB Fund Services
Harbor Capital Advisors Inc.	US Bancorp Asset Management, Inc.
Hartford Funds Management Company, LLC	VanEck Associates
Invesco	Wellington Management Company LLP
Lord, Abbett & Co. LLC	William Blair Investment Management
Macquarie Group	

* Sheltered Harbor and SIFMA were invited to observe the tabletop, representing critical custodian and sell-side relationships to ICI members. ICI continues to seek meaningful partnerships in cyber resilience and business continuity planning with relevant entities to the benefit of its members.



The Asset Management Industry
SERVING INDIVIDUAL INVESTORS

INVESTMENT COMPANY INSTITUTE

WASHINGTON, DC • BRUSSELS • LONDON • WWW.ICI.ORG