

ODD IN FOCUS: CYBERSECURITY RISK ASSESSMENT/TESTING PROGRAM



Operational Due Diligence (ODD) is a critical part of the manager selection process. One key area of ODD is understanding a manager's cybersecurity risk assessment and testing program. A cybersecurity risk assessment should be independently conducted with the goal of helping to identify and evaluate potential vulnerabilities within a manager's technology infrastructure.

WHY

- Cybersecurity risk assessments and testing are key components of an organization's risk management strategy. Without a good testing program, firms are at higher risk of having potential weaknesses exploited by cybersecurity hackers.
- Cybersecurity has received increased regulatory attention. For instance, the SEC has made cybersecurity a focus area in recent regulatory examinations. Failure to comply with the necessary cybersecurity rules can result in fines and reputational harm.

HOW

- The approach to managing cybersecurity risks varies with the size of the manager. Larger managers usually maintain dedicated internal resources, whereas smaller firms tend to outsource this function to various providers. Firms can follow the National Institute of Standards and Technology (NIST) cybersecurity framework, a set of guidelines to help organizations reduce cybersecurity risk.
- On an annual basis, investment managers should undergo a full evaluation of their IT systems and infrastructure. The cybersecurity risk assessment is an ongoing process that involves continuous monitoring to identify and mitigate any new risks and ensure the current controls are effective. These evaluations can include formal penetration tests, vulnerability assessments, policy and procedure reviews, or vendor due diligence and oversight.

ODD RISK POTENTIAL: HIGH

- A cybersecurity breach could result in the theft of personally identifiable information (PII), sensitive internet protocol (IP), confidential and/or proprietary information financial loss, reputational damage, regulatory penalties, and operational disruption.
- Even with robust cybersecurity controls in place, managers remain vulnerable to cybersecurity breaches and must establish documented policies and procedures for responding to potential cybersecurity incidents.
- Risk assessments will vary based on the manager's underlying infrastructure—i.e., whether the manager employs a cloud-based infrastructure or on-premise servers. For cloud-based managers, vulnerability and penetration testing is essential, since endpoints in these systems may have weaknesses. However, not all cloud-based managers consistently conduct this type of testing. Managers using their own servers are required to restrict and safeguard physical access to these servers, encrypt sensitive data, and perform regular backups to secure locations or data facilities.

The Cambridge Associates Business Risk Management Group contributed to this publication.

Published February 25, 2025

Manager Relevance

HEDGE FUND MANAGERS: Hedge fund managers may have complex trading strategies that rely on sophisticated trading systems and algorithms that need protecting. Such protection is crucial given the rapid pace of trading and nature of the strategies. If managers cannot access their systems, they will be unable to execute their strategies, leading to disruption in their investment activities.

PRIVATE FUND MANAGERS: Private fund managers handle sensitive business information and may have access to PII at underlying portfolio companies, exposing them to headline risk if a breach occurs. Implementing robust cybersecurity controls is crucial to safeguard their business and uphold investor trust. Private fund managers are also responsible for evaluating the cybersecurity controls in place at their underlying portfolio companies.

LONG-ONLY FUND MANAGERS: Given their long-term investments and substantial exposure to public markets, long-only fund managers are also at risk of hackers gaining access to their systems.

Key Control Review

#1 DOCUMENTATION OF POLICIES

- Written Information Security Plan (WISP) to address how the firm identifies, assesses, and mitigates cybersecurity risks. This document should contain guidelines regarding the timing and purpose of the firm's cybersecurity tests and assessments.
- Incident response plans can ensure managers effectively respond to and recover from cybersecurity incidents.
- Additional policies include access controls, data protection (GDPR), password policy, remote access policy, and an email security policy.

#2 TESTING

- Annual employee cybersecurity training and ad hoc simulated phishing testing.
- At least quarterly vulnerability scanning and annual penetration testing as a standard practice. Best practice is to rotate independent third-party cybersecurity consultants/providers to test the network every two years to gain fresh perspective and identify potential vulnerabilities.
- Active monitoring and due diligence of third-party vendors and subvendors to ensure they are meeting the organization's security standards.
- Security audits, such as security operations center reports to identify any gaps in the firm controls.
- Domain name testing to ensure that domain names link correctly to the proper IP addresses and to identify any spoofing attempts.

#3 GOVERNANCE AND OVERSIGHT

- Larger managers may have a cybersecurity committee that includes senior leaders such as the CISO/CTO, CIO, COO, CFO, CCO, risk manager, etc. The committee provides an objective process for addressing cybersecurity risks. By establishing committees and proper communication channels, the manager should be able to provide appropriate disclosures, timely notifications to clients, and effective remediation efforts in the event of an incident.
- Whether a manager has a cybersecurity committee or not, there should be clear and regular reporting procedures for testing results and remediation plans for any vulnerabilities or weaknesses detected.

Case Study: Hedge Fund 1 Manager

SUMMARY

Hedge Fund 1 (HF1) had a bad actor gain access to an employee email account after the employee fell for a phishing attempt. The bad actor was able to access PII through this email account, requiring HF1 to send a notice to all investors alerting them about the breach.

Ultimately, this incident caused reputational harm to HF1 as they had to notify clients of a known breach. While there did not appear to be any misuse of client or investor PII, this incident called into question the firm's commitment to protecting clients from cyber threats by investing in a robust cybersecurity program.

DESCRIPTION OF CONTROLS



The manager had enacted multi-factor authentication, had their IT provider conduct vulnerability scanning, and had employee training.



However, the firm did not have an independent party conduct the vulnerability scanning or penetration testing, which limited the efficacy of these assessments. It would have been a best practice to engage a truly independent party for these assessments.

Copyright © 2025 by Cambridge Associates. All rights reserved.

This report may not be displayed, reproduced, distributed, transmitted, or used to create derivative works in any form, in whole or in portion, by any means, without written permission from Cambridge Associates ("CA"). Copying of this publication is a violation of US and global copyright laws (e.g., 17 U.S.C. 101 et seq.). Violators of this copyright may be subject to liability for substantial monetary damages.

This report is provided for informational purposes only. The information does not represent investment advice or recommendations, nor does it constitute an offer to sell or a solicitation of an offer to buy any securities. Any references to specific investments are for illustrative purposes only. The information herein does not constitute a personal recommendation or take into account the particular investment objectives, financial situations, or needs of individual clients. Information in this report or on which the information is based may be based on publicly available data. CA considers such data reliable but does not represent it as accurate, complete, or independently verified, and it should not be relied on as such. Nothing contained in this report should be construed as the provision of tax, accounting, or legal advice. PAST PERFORMANCE IS NOT A RELIABLE INDICATOR OF FUTURE RESULTS. ALL FINANCIAL INVESTMENTS INVOLVE RISK. DEPENDING ON THE TYPE OF INVESTMENT, LOSSES CAN BE UNLIMITED. Broad-based securities indexes are unmanaged and are not subject to fees and expenses typically associated with managed accounts or investment funds. Investments cannot be made directly in an index. Any information or opinions provided in this report are as of the date of the report, and CA is under no obligation to update the information or communicate that any updates have been made. Information contained herein may have been provided by third parties, including investment firms providing information on returns and assets under management, and may not have been independently verified.

Cambridge Associates is a global group of companies that provide investment management, investment advisory, research, and performance reporting services. For the purposes of this document "us", "the Firm", "our", "we", "CA", "Cambridge Associates", and similar terms refer collectively to the following list of companies. Similarly, unless otherwise stated the figures provided are the combined total for the following list of companies: Cambridge Associates, LLC (a registered investment adviser with the US Securities and Exchange Commission, a Commodity Trading Adviser registered with the US Commodity Futures Trading Commission and National Futures Association, and a Massachusetts limited liability company with offices in Arlington, VA; Boston, MA; Dallas, TX; New York, NY; and San Francisco, CA), Cambridge Associates Limited (a registered limited company in England and Wales, No. 06135829, that is authorized and regulated by the UK Financial Conduct Authority in the conduct of Investment Business, reference number: 474331); Cambridge Associates GmbH (authorized and regulated by the Bundesanstalt für Finanzdienstleistungsaufsicht ('BaFin'), Identification Number: 155510), Cambridge Associates Asia Pte Ltd (a Singapore corporation, registration No. 200101063G, which holds a Capital Market Services License to conduct Fund Management for Accredited and/or Institutional Investors only by the Monetary Authority of Singapore), Cambridge Associates Limited, LLC (a registered investment adviser with the US Securities and Exchange Commission, an Exempt Market Dealer and Portfolio Manager in the Canadian provinces of Alberta, British Columbia, Manitoba, Newfoundland and Labrador, Nova Scotia, Ontario, Québec, and Saskatchewan, and a Massachusetts limited liability company with a branch office in Sydney, Australia, ARBN 109 366 654), Cambridge Associates Investment Consultancy (Beijing) Ltd (a wholly owned subsidiary of Cambridge Associates, LLC which is registered with the Beijing Administration for Industry and Commerce, registration No. 110000450174972), Cambridge Associates (Hong Kong) Private Limited (a Hong Kong Private Limited Company licensed by the Securities and Futures Commission of Hong Kong to conduct the regulated activity of advising on securities to professional investors), and Cambridge Associates AG (a Swiss Limited Company, registration number CHE-115.905.353, that is authorized and Regulated by the Swiss Financial Market Supervisory Authority (FINMA)).