Registered Investment Advisors and Funds: The Time to Enhance Your Cybersecurity Program is Now

By Thomas J. DeMayo, Principal, Cybersecurity and Privacy Advisory and Victor Peña, Partner-Financial Services

The Securities and Exchange Commission (SEC) on February 9, 2022 voted to propose significant changes to how Registered Investment Advisors (Advisors) and Investment Companies (Funds) manage their cybersecurity risk and disclose significant cyber-related incidents to the SEC. The proposals would issue new cybersecurity-specific rules under the Investment Company Act of 1940 and the Investment Advisers Act of 1940.

The proposals are in response to the escalating cybersecurity risks faced by Advisors and Funds and the increased sophistication of the attacks by cyber threat actors. Further, the SEC believes that the existing regulations to which Advisors and Funds are subject do not directly address the current cyber threats. This puts them at risk of suffering significant financial, operational, legal and reputational harm. Ultimately, these incidents can cause substantial harm to Advisors' and Funds' clients and investors.

SEC Cybersecurity Concerns

In the proposals, the SEC notes the following major cybersecurity concerns*:*

- What the SEC views as a lack of desire of Advisors and Funds to implement effective cyber-risk management programs placing clients and investors at risk. This concern stems specifically from the SEC observing a number of practices where Advisors and Funds continue to disregard the SEC's observations and recommendations to bolster cybersecurity programs.

- Cybersecurity disclosures by Advisors and Funds are not sufficient to allow clients and investors to make informed investment decisions.

- Currently, cybersecurity incidents are not required to be reported to the SEC resulting in insufficient oversight and understanding of the cyber risks faced by Advisors and Funds and the overall impact to capital markets and investors.

SEC Proposals

To address their concerns, the SEC is proposing the following amendments.

Cyber risk-management rules and procedures would need to be formally defined, documented, adopted, and implemented to require the following elements:

- ***Risk Assessment*** – A formalized and documented risk assessment would need to be performed on a consistent basis. The risk assessment would need to inventory and rank the risks faced directly by the Funds and Advisors as well as the risks associated with their Service Providers.

- ***User Security and Access*** – Advisors and Funds would be required to:

    - Establish acceptable use policies to govern and guide user behaviors.

- Identify and authenticate individual users, inclusive of multi-factor authentication.
- Remove access in a timely manner when circumstances warrant it.
- Restrict access based on a need-to-know and need-to-perform basis.
- Secure remote access.

- ***Information Protection*** – Advisors and Funds would need to categorize the risks of the information they process and implement effective controls relative to those risks.

- ***Threat and Vulnerability Management*** – An effective program would need to be created and maintained to effectively detect, mitigate, and remediate threats and vulnerabilities before they result in harm.

- ***Cyber Incident Response and Recovery*** – Incidents will occur. Advisors and Funds would need effective plans and strategies to identify, respond, and recover from cyber incidents.

Annual Report on Cybersecurity Program

On an annual basis, Funds and Advisors would need to assess the design and operating effectiveness of their cybersecurity program in a written report (the Report). The Report would need to be created to describe the assessment performed, the controls tested, and the results thereof. Further, the Report would need to acknowledge any incidents that occurred since the last report and any changes to the cyber policies and procedures. This would likely require Advisors and Funds to seek outside professional help.

Added Governance

Additional governance and oversight would be required. A Fund's Board of Directors (the Board) would need to be actively involved in the establishment and ongoing review of the cybersecurity program. The Board would be required to review and approve a Fund's cybersecurity policies and procedures. Further, to ensure ongoing oversight, the Board would need to be provided and review the completed Report (noted above).

Maintenance of Additional Records

As an extension of the Books and Records Rule and Investment Company Act, the following cybersecurity-related items would be required to be maintained for a five-year period:

1. A copy of the cybersecurity policies and procedures that are in effect at any time within the past five years.
2. A copy of the written report documenting the annual review of its cybersecurity policies and procedures.
3. A copy of any Form ADV-C filed.
4. Records documenting the occurrence of any incident and the associated response and recovery efforts.
5. Records documenting the performance of the cybersecurity risk assessment.

Incident Disclosure

Incident disclosure requirements would be introduced to require disclosures to the SEC within 48 hours of a confirmed incident.

Cyber risks and incidents would also need to be disclosed in the brochures provided to clients and investors. Further, in the event of an incident, an Interim Brochure needs to be released to existing clients including the disclosure of the incident.

Recommendation

Based on the current Administration and the nature of the risks identified and described in the SEC's proposals, we believe that it is probable that many of the proposed amendments will be adopted. Advisors and Funds should begin to assess the impact that the additional requirements would have on their organizations. Further, Advisors should consider consulting with their cybersecurity professionals on what an adoption plan would look like in order to begin to plan for time and resources accordingly.

Contact Us

At PKF O'Connor Davies, LLP, we have a team of dedicated cybersecurity and privacy experts that can help Funds or Advisors establish and maintain an effective cybersecurity program that will meet the SEC's requirements. We encourage you to visit Cybersecurity & Privacy Advisory for a complete listing of our services.

For more information on these SEC cyber proposals, please contact your engagement team or:

Thomas J. DeMayo, Principal
Cybersecurity and Privacy Advisory
CISSP, CISA, CIPP/US, CRISC, CEH, CHFI, CCFE
tdemayo@pkfod.com

Victor Peña, CPA
Partner
Financial Services
vpena@pkfod.com

Michael Provini, CPA
Partner
Financial Services
mrpovini@pkfod.com

www.pkfod.com

About PKF O'Connor Davies

PKF O'Connor Davies, LLP is a full-service certified public accounting and advisory firm with a long history of serving clients both domestically and internationally. With roots tracing to 1891, the Firm has 16 offices in New York, New Jersey, Connecticut, Maryland, Massachusetts, Florida and Rhode Island and more than 1,200 professionals providing a complete range of accounting, auditing, tax and management advisory services. PKF O'Connor Davies is led by over 135 partners who are closely involved in the day-to-day management of engagements, ensuring a high degree of client service and cost effectiveness.

The Firm is a top-ranked firm, according to *Accounting Today's* 2021 "Top 100 Firms" list and was recently recognized as one of "America's Best Tax Firms" by *Forbes*. PKF O'Connor Davies was named one of *Vault's* 2022 Accounting 50, a ranking of the 50 best accounting employers to work for in North America and ranked among the top 50 most prestigious accounting firms in America in a complementary *Vault* survey.

PKF O'Connor Davies is the lead North American representative of the international association of PKF member firms. PKF International is a network of legally independent member firms providing accounting, tax and business advisory services in over 400 locations in 150 countries around the world. With its tradition, experience and focus on the future, PKF O'Connor Davies is ready to help clients meet today's ever-changing economic conditions and manage the growing complexities of the regulatory environment. For more information, visit www.PKFOD.com.