Proskauer

Cybersecurity Continues to be a Focal Point for Regulators in 2024

The Capital Commitment on **April 18, 2024**

The SEC's new and proposed rules on cybersecurity and cyber-incident reporting will have a dual impact on private investment advisers and funds.

First, the proposal by the SEC will impose cybersecurity related obligations on investment advisers, registered investment companies and business development companies, with a final rule in this sector (the "adviser cybersecurity rule") expected in April 2024.

Second, the already promulgated Rule on cyber security and incident reporting by public companies adopted in July 2023 (the "corporate cybersecurity rule") will increase scrutiny into, and comparison of, companies' cybersecurity programmes by investors, insurers and the public, as well as by the regulator itself.

As with any new rules, increased enforcement is anticipated, but the biggest change we expect is one of mind-set and scope. Although the Commission has explained that it is not "*seeking to prescribe particular cybersecurity defenses, practices, technologies, risk management, governance, or strategy*", comparison is inevitable and market standards will naturally become more comprehensive and sophisticated. In fact, the Commission considers a key driver of the obligation to give investors and shareholders consistent and up-to-date information about cyber risks and to allow market participants to compare themselves with their peers. We therefore anticipate a market wide shift in awareness of and focus on cybersecurity issues.

The 2024 Cybersecurity Benchmarking Survey, a joint project of ACA Group and the Nationals Society of Compliance Professionals, reported responses of compliance professionals at 308 investment advisor firms who participated in the survey. The survey yielded notable findings in several areas of interest including regulatory preparedness. Regarding the new SEC cybersecurity rules (already promulgated and proposed), the primary concerns expressed were uncertainty about how the rules will be enforced and compliance with the incident reported requirements and timeframes.

As cybersecurity risks rise with increasing dependence on electronic systems, as well as (in the words of SEC Director Erik Gerding) "*the growth of remote work, the ability of criminals to monetize cybersecurity incidents, the use of digital payments, and the increasing reliance on third party service providers*" for cloud and other IT services, costs of these incidents are rising also – for the companies and for their investors. The global average cost of a data breach in 2023 was US$4.5m, and in the US is $9.48m, according to an annual report produced by IBM.

The two rules – with one applying to public companies and the other to investment advisers – share core obligations: to report significant cybersecurity incidents within a very short period, to provide fuller cybersecurity-related disclosures, to require boards to demonstrate effective supervision, and new policy, procedure and recordkeeping requirements. Yet there are key differences between the current adviser related proposal and the public company rule:

- From December 18, 2023, public companies must disclose on Form 8-K all "material" cybersecurity incidents within *four business days* of determining materiality (which assessment must be made without undue delay).
- The proposed rule for advisers reflects their fiduciary role: to file a report *within 48 hours* of concluding (or having reasonable basis to conclude) that a significant *adviser* or *fund* cybersecurity incident has occurred or is occurring.
- A significant cybersecurity incident is defined in relation to an adviser as one impacting the adviser, the fund it manages or one of the investors in the fund – namely one that "*significantly disrupts or degrades the adviser's ability, or the ability of a private fund client of the adviser, to maintain critical operations, or leads to the unauthorized access or use of adviser information, where the unauthorized access or use of such information results in: (1) substantial harm to the adviser, or (2) substantial harm to a client, or an investor in a private fund, whose information was accessed*."

The SEC's approach to the new and proposed rules, that of requiring greater focus on. and board level attention to. cyber resilience echoes that of regulators worldwide. In the UK, a draft code of practice on cyber security governance and an accompanying consultation was launched in January 2024 as part of the UK Government's National Cyber Strategy. The draft code, which will be voluntary but is designed to help businesses meet their existing legal and regulatory obligations, emphasizes the need for a top-down approach to cyber governance and focuses on ensuring entities have detailed and robust plans in place not just to respond to cyber incidents but to recover effectively and promptly from them.

In the US, these new SEC requirements will impact insurance coverage, as public disclosures of cyber security policies and procedures will enable insurance companies better to assess companies and advisers against their peers when setting premiums. The scope and cost of cyber-insurance will be a key part of any in scope entity's cyber risk assessment and, in turn, its disclosures.

To ensure compliance with the proposed rule, private fund advisers will need to ensure that effective cyber risk management regimes, with incident response planning and escalation that allows timely appropriate reporting, are deeply integrated into business planning. This will involve coordination across multiple functions (risk, finance, legal, IT security, audit and communications/ public relations to name just a few). Data collection will be crucial, as will weeding out false positives (an area in which AI may provide some help). One thing is certain, the risks around cybersecurity continue to grow and with it, the focus of regulators on rule compliance.

Read more of our Top Ten Regulatory and Litigation Risks for Private Funds in 2024.

View original.

Related Professionals

- **Margaret A. Dale**
  Partner
- **Mike Hackett**
  Partner

- **Stephen Hibbard**
  Partner
- **Timothy W. Mungovan**
  Chairman of the Firm
- **Joshua M. Newville**
  Partner
- **Todd J. Ohlms**
  Partner
- **Robert Pommer**
  Partner
- **Seetha Ramachandran**
  Partner
- **Jonathan M. Weiss**
  Partner
- **Julia D. Alonzo**
  Litigation Department Legal Director
- **William D. Dalsen**
  Partner
- **Kelly M. McMullon**
  Special International Labor, Employment & Data Protection Counsel
- **James Anderson**
  Partner
- **Adam L. Deming**
  Senior Counsel
- **Adam Farbiarz**
  Senior Counsel
- **Reut N. Samuels**
  Associate
- **Hena M. Vora**
  Associate