Danforth Advisors

Life Sciences, Well Run.

New SEC Reporting Rules for Cyber Security Will Take Effect in December 2023

Here's What Public Biotech Companies Need to Know

The SEC released a final rule on cyber security and reporting requirements for public companies on July 26, 2023. In addition to reporting all material cyber security incidents to the SEC, the regulation calls for disclosure of cyber security risk management, strategy and governance.

Below is a quick reference guide for public biotech companies. Danforth's risk management and information security consultants can provide advisory or operational execution of the steps required to achieve compliance.

Reporting Requirements

Incident Reporting

- Disclosures must occur within four business days after the company determines that a material cyber security incident has occurred. The trigger is the date upon which the company determined the incident was material, not the actual date of the incident. This is to be done through the 8-K section 1.05.
- The incident may be a single event or multiple related events which, when aggregated, could give rise to a material exposure.
- The report must describe the incident's nature, scope, timing and impact on the organization.
- The disclosure must also include incidents on vendors' or suppliers' networks if they involve company information.

Ongoing Reporting

- All public companies must report in the 10-K how they assess, identify and manage material cyber security threats to the organization.
- Disclose integration of all processes with overall risk management.
- Disclose engagement of any outside third parties to assist with cyber security.
- Describe the Board of Directors' role in oversight of cyber risk: which part of the Board addresses risk (i.e., full Board, audit committee, special risk committee, etc.) and the role and expertise of management in assessing/managing cyber risk.
- Disclose how the Board is informed of risks.

Compliance Dates

- All reporting is to begin December 18, 2023. Smaller companies will be given extra time to start reporting, with an effective date of June 15, 2024.
- The 10-K reporting will be required for annual reports for fiscal years ending on or after December 15, 2023.

Action Steps

- Update or create cyber security materiality assessments into incident response plans.
- Review all applicable insurance policies to determine if an SEC report will also trigger a report to the insurance carrier.
- SEC filings should track with information being provided to insurance carriers in applications, corporate contracts regarding cyber security and website disclosures.
- Ensure internal alignment of legal, IT, finance, communications, investor relations and risk management personnel so as not to contradict each other with public statements or documents.
- Ensure compliance with additional, preceding cyber security regulations:
    - 1996 | Heath Information Portability and Accountability Act (HIPAA)
    - 1999 | Gramm-Leach Bliley Act
    - 2002 | Homeland Security Act

The number one rule of cyber security is to treat everything as vulnerable. Danforth's risk management and information security specialists are available to help in a flexible, interim or project-based way.

Contact: Ed Downey, Head of Risk Management Consulting | 617-631-7979 | edowney@danforthadvisors.com