Cybersecurity Incident Disclosure Program

Supporting SEC Compliance with Cybersecurity Risk Management, Strategy, Governance and Incident Disclosure.

intra systems Advisory Division

Understanding the New Rules

On July 26, 2023, the Securities and Exchange Commission adopted new requirements to enhance and standardize disclosures related to cybersecurity risk management, strategy, governance, and incident response for public companies subject to the Securities Exchange Act of 1934.

These new reporting regulations require that companies provide annual disclosures of cybersecurity risk management, strategy, and process governance via the 10-K. Beyond reporting annually as to a firm's cybersecurity strategy and the role of management and the Board in executing and governing the strategy, companies must also disclose any material incidents via an 8-K.

The journey to SEC compliance and preparedness begins with IntraSystems Advisory Division. Our comprehensive 3-phased approach was designed to fortify your organization's cybersecurity posture and ensure SEC compliance.

Approach & Solution Roadmap

Our approach was designed to help minimize the complexities of developing a compliance program, while integrating the requirements seamlessly into your business operations.

1

PHASE 1
Response Foundations and Validation

- Develop / review / finalize and validate Incident Response Plan.
- Develop template 8-K for disclosing material incidents.
- Validate Incident Response Plan via tabletops.
- Assess and benchmark the maturity of the existing client cybersecurity program.
- Test and validate client ability to generate an 8-K within four days of the detection of a material incident through tabletop exercises.
- Establish a platform for incident tracking and response.
- Perform Business Impact Analysis to inform Cybersecurity Strategy.
- Develop template 10-K to satisfy annual reporting requirements.
- Develop cybersecurity strategy.

2 PHASE 2
Execution and Refinement

- Execution of defined strategy.
- Continued tabletop exercises to refine Incident Response Plan and ensure ability to execute the plan.
- Test client's ability to identify breaches and properly evaluate their materiality.
- Monitor compliance with policies and standards specific to the management of cybersecurity
- Perform regularly scheduled risk assessments on the highest impact areas of the business.
- Update and communicate progress on the execution of cybersecurity strategies to management and the Board.
- Provide the Board with training to address knowledge gaps required to enable ongoing governance.

3 PHASE 3
Integration and Futureproofing

- Integrate the business into cybersecurity strategy, detection, and response.
- Define automated vs manual execution of processes and controls.
- Provide defined and regularly delivered updates addressing the cybersecurity program, risks, and incidents to management and Board.
- Continue to update 10-K as the program progresses, managing compliance with the addition of risk.
- Integrate cybersecurity into financial and strategic planning.

Benefits of IntraSystems Advisory Division Approach

Maximize Focus

Enable focus on initiatives that matter via a business-aligned IT strategy and executable roadmap.

Justify Strategy

Develop business cases with detailed BAU and target-state financial models.

Purposefully Execute

Equip your team with a detailed architecture and implementation plan, with resources to execute.

Ensure Adoption

Drive the success of the program via organizational change management.