Compliance with the SEC Cybersecurity Rules

On July 26, 2023, the Securities and Exchange Commission (SEC) adopted new cybersecurity rules intended to better equip investors to evaluate an organization's exposure to cybersecurity risks and incidents, as well as their ability to mitigate those risks. The changes require that firms provide investors with consistent and comparable information pertaining to incident reporting, process disclosures, and management's role in assessing material cybersecurity risks. All companies listed in U.S. exchanges, including foreign private issuers, must provide these disclosures beginning with annual reports for fiscal years ending on or after December 15, 2023. Smaller reporting companies have an additional 180 days to provide disclosures.

What are the New Requirements?

Incident Reporting Disclosure

Organizations will be required to report the material impact of cybersecurity incidents and data breaches on Form 8-K within four business days, with an exception for disclosures that could pose risk to national security or public safety. They will also need to provide information and updates regarding previously disclosed incidents on Form-20-F. The requirements further add "cybersecurity incidents" as a reporting topic on Form 6-K.

Risk Management, Strategy, and Governance Disclosure

Organizations must include their cybersecurity risk management, strategy, and governance as part of their annual report in Form 20-F. The required key controls include security risk assessments; access controls; continuous monitoring; detection & response; vulnerability management; and vendor risk management. Form 20-F will also include standardized disclosure of management's oversight of cybersecurity risk, whether cybersecurity is included as part of the business strategy, financial planning, and management's role and expertise in assessing cybersecurity risk.

HOW FTI CYBERSECURITY CAN HELP

Mature and effective cyber programs and processes can serve as a market differentiator and value-add for organizations, attracting investors. FTI Cybersecurity will work with your organization to ensure all SEC cybersecurity requirements are met while maximizing your return on cybersecurity investment.

FTI Cybersecurity understands the intersection of security, risk, and financial disclosures. Our experts can help prepare required disclosures based on your program and risk strategies, including the annual report.

FTI Cybersecurity uses a strategic approach to assess the cybersecurity challenges affecting your organization and prepare you to comply with regulations and respond to incidents, including implementing technical solutions that are integrated with traditional cybersecurity risk management.

FTI Cybersecurity can help you prepare for timely incident response and disclosures through reviewing existing incident response plans and conducting table-top exercises to stress test your organization's ability to respond in light of these new rules.

OUR SERVICES

Strategic Advisory & Education

FTI Cybersecurity serves as a strategic partner to management, providing insight and guidance to help drive cybersecurity program maturity, risk management, governance, and resilience. Understanding cybersecurity's value helps ensure proper protections are implemented, mitigating risks and protecting investments, reputation, and corporate value.

Cybersecurity Stakeholder Engagement

FTI Cybersecurity will inform engagement between the Board and other stakeholders to ensure alignment on cybersecurity priorities and consistent understanding of security initiatives and investments.

Cybersecurity Strategy

Our team can provide guidance on cybersecurity strategies, such as third-party risk mitigation, incident response, and regulatory compliance. We align cyber risk management with business needs by identifying how cyber risk management and resilience help achieve business objectives.

Incident Response

We work in conjunction with your organization or as a separate unit to support your incident response efforts, before and after incidents occur.

Preparation

Being ready for cyber threats is fundamental to the success of your incident response program. This phase involves establishing and training an incident response team and developing appropriate tools and resources you will need for each aspect of incident response.

We work with your business to select and implement controls based on the results of our risk assessments to limit the number of potential incidents your organization may face. We also facilitate the execution of incident response exercises and tabletops to prepare teams for timely response and reporting.

Detection & Analysis

Residual risk inevitably persists after controls are implemented. Early steps to identify, detect, and analyze threats facing your networks are key to developing effective containment and eradication strategies. Once an incident is identified, we combine the resources and tools necessary to determine the scope, impact, and appropriate response. These efforts determine the source of the incident and preserve necessary forensic artifacts.

Data Identification & Review

Our comprehensive review enables clients to continue daily business operations in a post-breach environment, with assurance that the task is being handled expeditiously, sensitively, and competently. We regularly conduct reviews in multiple formats and languages, and our team's expertise ensures important information will not be overlooked, allowing for remediation, regulatory compliance, and accurate document preparation.

Cybersecurity Program Maturity Assessment

A comprehensive cybersecurity program is critical in today's threat landscape. To ensure your organization is properly protected, our team will determine if you meet industry standard best practices, identify and assess your vulnerabilities, and devise a holistic set of scored recommendations. Our complete cybersecurity program assessment includes:

Policies, Procedures, Staff Gap Analysis and Design

Our experts perform a thorough review of security policies and procedures; conduct interviews with staff to understand how security policies, processes, and procedures are implemented, managed, and enforced; and administer a gap assessment of existing security controls as compared to industry standards.

Disclosure Preparation

Our experts will help you translate internal cybersecurity policies and procedures into effective confidence-building risk management, strategy, and governance disclosures that will both meet SEC disclosure requirements and build investor trust.

Penetration Testing

Knowing whether your critical assets are at risk is key in strengthening your infrastructure. This assessment simulates an attacker both with and without familiarity of your infrastructure and tests your external and internal IT systems for any vulnerabilities that could be used to disrupt the confidentiality, availability, or integrity of your network.

Vulnerability Assessments

Our experts design custom vulnerability assessment plans to ensure your infrastructure is secure and stable, preventing hackers from infiltrating systems with unidentified and unpatched vulnerabilities. Regular assessments allow our team to test systems for any irregularities, inconsistencies, and anomalies that might render an organization's network vulnerable to attack.

WHY FTI CYBERSECURITY

Multidisciplinary Expertise

— Intelligence-led, expert-driven, strategic approach to cybersecurity challenges

— Core team from intelligence agencies, law enforcement, and global private sector institutions

Globally Positioned

— Ability to respond anywhere in the world

— Ability to staff the largest and most complex engagements and investigations

— Relationships with the top global intelligence agencies, regulatory authorities, and private agencies

Integrated & Comprehensive

— Comprehensive services include crisis communications, e-discovery, forensic investigations, and more

— Seamless integration of FTI Consulting's expertise across service offerings

ANTHONY J. FERRANTE
Global Head of Cybersecurity
Senior Managing Director
+1 202 312 9165
ajf@fticonsulting.com

JORDAN RAE KELLY
Head of Cybersecurity, Americas
Senior Managing Director
+1 202 312 9140
jordan.kelly@fticonsulting.com

08312023 | VN02724-v03