Network Security Regulation SEC

Author: Dr. Jamal Thompson, PhD

The U.S. Securities and Exchange Commission (SEC) enforces several laws and regulations that require IT vendors and companies to secure client data, particularly when it involves financial information. The most relevant regulations include:

1. Regulation S-P (Privacy of Consumer Financial Information)

- **Overview**: Requires financial institutions under SEC jurisdiction to adopt written policies and procedures to protect the confidentiality and security of customer information.
- **Key Requirements**:
  - Protect customer records and information against unauthorized access or threats.
  - Notify customers about how their information is collected, used, and shared.
  - Provide customers with the ability to opt out of sharing personal data with third parties.

2. Regulation SCI (Systems Compliance and Integrity)

- **Overview**: Applies to financial market participants, such as brokers, dealers, and IT vendors supporting these entities. It mandates robust IT system security to ensure the integrity of financial systems.
- **Key Requirements**:
  - Establish policies and procedures for the capacity, integrity, resiliency, and security of IT systems.
  - Report significant IT system disruptions, breaches, or vulnerabilities to the SEC.

3. Cybersecurity Risk Management Guidance

- **Overview**: The SEC has issued guidance emphasizing that companies must disclose cybersecurity risks and incidents to investors, including how they protect data.
- **Key Points**:
  - Companies should maintain effective cybersecurity policies and procedures.

- Public companies must disclose material cybersecurity risks or breaches in their filings.

4. Sarbanes-Oxley Act (SOX)

- **Overview**: While primarily focused on financial reporting, SOX includes provisions for IT systems that store financial data.
- **Key Requirements**:
  - Establish internal controls for financial reporting and safeguard against unauthorized data access.
  - Ensure proper data management, access logs, and IT audit trails.

5. Investment Advisers Act Rule 206(4)-7

- **Overview**: Requires registered investment advisers to adopt policies and procedures to protect client information and prevent breaches.
- **Key Points**:
  - Implement written policies to mitigate cybersecurity risks.
  - Regularly review and assess the effectiveness of security measures.

6. Gramm-Leach-Bliley Act (GLBA) – Safeguards Rule

- **Overview**: Although overseen by multiple regulators, the SEC enforces GLBA rules for financial institutions under its jurisdiction.
- **Key Requirements**:
  - Develop, implement, and maintain a comprehensive information security program.
  - Assess risks to customer data and implement safeguards to address them.

Non-Compliance Consequences

Failure to adhere to these SEC regulations can result in:

- Fines and penalties.
- Legal liabilities from breaches.
- Reputational damage.

Sincerely,

Dr. Jamal Thompson

616 Cypress Creek Pkwy Suite 250 A, Houston, TX. 77090, Office: 346-998-2347 Email: drthompson@drjamalthompson.com

Publishing Rights

For permission requests, write to:
Dr. Jamal Thompson
616 Cypress Creek Pkwy Suite 250 A
Houston, TX 77090
Email: Drthompson@drjamalthompson.com