BUSINESS INFORMATICS

A Practice Group by SingerLewak

SEC CYBERSECURITY GOVERNANCE AND DISCLOSURE RULES

SingerLewak's Roadmap to Compliance

Timely SEC Cybersecurity Rules – what's at stake? In short, it's time to disclose how well your organization governs and manages its material Cybersecurity risks, threats, and incidents. How soon? For fiscal years ending post-12/15/23 (and, if you are pre-IPO... be prepared)

Regulatory Highlights

The rules focus on 3 key disclosures:

- **Cyber Risk Management**
  How you assess, identify and manage material risks from Cybersecurity threats – and determine how possible and previous incidents can impact your organization. (S-K)
- **Cyber Incident Reporting**
  Disclosure of known material incidents (typically) within 4 business days with reference to the incident's impact on your operations and financial condition. (8-K)
- **Cyber Governance**
  How your board's oversight processes of Cybersecurity risks and your management's role and expertise in governing Cybersecurity. (S-K)

Subject Matter Professionals

Cybersecurity and technical accounting professionals ready to help, playing either of 2 roles:

- **Role 1**
  Hands-on, skilled Cyber and SEC accounting technical support to establish processes designed to help build your capability to comply with these rules.
- **Role 2**
  Seasoned, skilled Cyber and SEC accounting eyes to assess your compliance posture.

Bob Green, CPA.CITP, CGMA
Partner | Practice Leader
Bgreen@singerlewak.com

Carl Grifka, CISSP, CISM, CISA
Managing Director
IT Risk & Assurance
Carl.Grifka@Singerlewak.com

Eric Rockwell, CISSP
Lead | Cybersecurity
ERockwell@Singerlewak.com

LET'S WORK TOGETHER

- Evaluate the readiness of your Cybersecurity program for SEC compliance.
- Develop a SEC Cybersecurity compliance roadmap for remediation of policies, controls, governance and behavior, supporting a more mature Cybersecurity posture and capability for incident and response management. Implement roadmap improvements, over time.
- Perform periodic, deeper evaluations of your organization's Cybersecurity "maturity level" as measured against established frameworks (e.g.; CIS and NIST).
- Ensure that your management team and your Board understand their roles in the oversight and management of Cybersecurity risks and threats.