RISK & ACCOUNTING ADVISORY SERVICES

Cybersecurity Risk Management & Incident Response Services

Whether responding to SEC requirements, or positioning your company to avoid cyber threats, a more formal structure to report back to key leadership and stakeholders on the maturity and governance of your cyber program is a must.

Enhancing Cybersecurity Measures to Respond to SEC Reporting Requirements

Recently, the Securities and Exchange Commission ("SEC") proposed amendments to enhance disclosures regarding cybersecurity risk management and incident reporting by public companies—emphasizing the increasing importance of cybersecurity in the realm of corporate governance as cyber-attacks become more frequent and sophisticated. Specifically, these new rules are designed to standardize and fast-track the information companies disclose around cybersecurity risks to investors, with the goal of providing an increased level of transparency.

Understanding the Proposed Amendments

Once enacted, these proposed rules will bring significant changes for public companies within their cybersecurity, risk management and corporate governance programs. At a high level, the new proposed rules would require:

- Reporting on cybersecurity incidents within four business days after it is determined that a material cybersecurity incident has occurred
- Regular disclosures around policies that identify and manage cybersecurity risks

- Disclosure about the Board of Directors' cybersecurity expertise and leadership's role in implementing cybersecurity governance practices
- Updates about prior material cybersecurity incidents and their related remediation efforts
- The reporting of cybersecurity disclosures via Inline eXtensible Business Reporting Language (Inline XBRL)
- If a cybersecurity incident occurs, organizations will need to comply with more stringent and timely reporting requirements to meet these new obligations. Examples of the information that will likely be needed include:
- The type of data that was stolen, accessed, and/or used for unauthorized purposes
- What impact the incident may have had on operations
- When the incident was discovered and what the investigation and remediation process was post-incident
- Impacts on current operations and/or relevant third parties

Cherry Bekaert
Your Guide Forward

We Can Help You Prepare

Cherry Bekaert's Information Assurance & Cybersecurity practice can help provide guidance to navigate these upcoming requirements, as well as protecting your company from cyber threats. We can help you to:

- Build (or fine-tune) your formal incident response policy so employees have a clear framework for detecting and reporting cybersecurity incidents within the updated timeline requirements
- Create a documented process for tracking and reporting on incident remediation efforts
- Re-examine disclosure procedures to alignment with the new rules
- Develop clear cybersecurity risk management procedures to align with overall risk management framework

Cyber Risk Management Service Offerings

We help organizations build cyber and business resiliency programs by providing an increasing level of protection against data loss, corruption, ransom, or other malicious attacks, and include strategic business continuity consulting, incident response, and risk management to ensure your business keeps running. To help you understand and navigate this ever-changing landscape, our Information Assurance & Cybersecurity professionals offers with the following cybersecurity solutions:

- Cybersecurity / IT Risk Assessment
- Cyber Framework Gap Assessments
- Cyber Program Evaluations
- Secure Architecture Assessments
- Identity and Access Management Assessments
- Vulnerability Assessment
- Penetration Testing
- Incident Response & Recovery Plan
- Third-Party and Supply Chain Management
- SOC and other Attest Readiness and Reporting
- User Awareness Training

Experience the Cherry Bekaert Difference

Every organization is different, but likely the best place to start is with a detailed evaluation of the maturity of your cyber governance program and your cyber risk assessment process, as well as a review of your security architecture, third-party risk management processes, and your incident response program.

Let Us Guide You Forward

Steven J. Ursillo, Jr. CPA, CISA, CISSP, CCSFP
Partner, Risk & Accounting Advisory Services
Information Assurance & Cybersecurity Leader
sursillo@cbh.com

cbh.com/riskadvisory

About Cherry Bekaert

"Cherry Bekaert" is the brand name under which Cherry Bekaert LLP and Cherry Bekaert Advisory LLC, independently owned entities, provide professional services in an alternative practice structure in accordance with applicable professional standards. Cherry Bekaert LLP is a licensed CPA firm that provides attest services, and Cherry Bekaert Advisory LLC and its subsidiary entities provide tax and advisory services. For more details, visit **cbh.com/disclosure.**

v. December 13, 2022 7:06 PM Brochure_RAAS_Cybersecurity-Risk-Management-Incident-Response-Services_874300751

Cherry Bekaert
Your Guide Forward