Date

The Coming SEC Cybersecurity Rules

Presented by:

Randy V. Sabett, J.D., CISSP
Cooley LLP

Kamran Salour
Lewis Brisbois

Privacy+ Security Forum

Cooley

LEWIS BRISBOIS

Speakers

Privacy+ Security Forum

Randy V. Sabett
Special Counsel
Cooley LLP

Cooley

Kamran Salour
Partner
Lewis Brisbois LLP

LEWIS BRISBOIS

Summary of cybersecurity disclosure requirements

- October 2011: SEC issued guidance on how cybersecurity risks and incidents should be disclosed
- February 2018: SEC issued guidance regarding disclosures of cybersecurity risks, procedures to keep management informed, and disclosure controls, reinforcing and expanding the 2011 guidance
- June 2021: SEC announced that it would focus on cybersecurity disclosures
- June and August 2021: SEC announced two settlements in actions related to cybersecurity disclosure control failure and data security incident (see next slide)
- March 2022: SEC announced proposed rules and opened comment period
- May 2022: comment period ended
- April 2023: expected final action on rules

SEC enforcement landscape

Privacy+ Security Forum

- **Cybersecurity disclosures.** In June 2021, the SEC announced that it would focus on cybersecurity disclosures made by public companies as part of its regulatory agenda; the SEC had previously issued guidance in 2018 and 2011 regarding disclosures of cybersecurity risks and disclosure controls
- **Enforcement actions.** Shortly thereafter the SEC filed in quick succession two public company cybersecurity enforcement actions, signaling an increase in cybersecurity enforcement
  - Notably, neither case included any indication that the companies or their executives intended to deceive investors or that either cybersecurity incident was material to investors, indicating that no intent to deceive is needed and that materiality will be measured qualitatively
  - Both cases involved an alleged failure to maintain adequate disclosure controls and procedures, highlighting the importance of companies' policies and procedures around cybersecurity
- **New proposed cybersecurity disclosure rules.** In March 2022, the SEC proposed new rules for cybersecurity disclosure and incident reporting

Details of enforcement developments

Privacy+ Security Forum

- In June 2021, the SEC settled with First American for what the SEC found were inadequate disclosure controls and procedural violations revealed in connection with a cybersecurity vulnerability
  - **Key takeaway**: implementation of reporting procedures designed to inform senior management of vulnerabilities that may be material for financial reporting purposes
- In August 2021, the SEC settled with Pearson plc for what the SEC found to be negligence-based fraud and disclosure controls deficiencies. Three months after learning an incident, Pearson submitted a filing to the SEC containing a cybersecurity related risk factor but made no mention of the intrusion and instead phrased the risk as a hypothetical risk.
  - **Key takeaway**: consistent with their relevant guidance, the SEC expects public companies to tailor their cybersecurity-related risk factors

Proposed Disclosure Requirements

Privacy+ Security Forum

Disclosure Item	SEC Form(s)	Summary
Reporting of material cybersecurity incidents (Form 8-K Item 1.05)	8-K	• Disclosure required where registrant experiences a cybersecurity incident that is determined to be "material" • Current report on Form 8-K due within four business days of **date of determination of materiality**
Material updates to cybersecurity incidents (Reg. S-K Item 106(d))	10-K, 10-Q	• Requires registrant to disclose any material changes, additions or updates to cyber incident previously disclosed on a Form 8-K • Requires registrant to disclose when a series of previously undisclosed individually immaterial cybersecurity incidents become material in the aggregate
Risk Management and Strategy (Reg. S-K Item 106(b))	10-K	• Requires registrant to describe its policies and procedures, if any, for the identification and management on cybersecurity risks
Governance (Reg. S-K Item 106(c))	10-K	• Requires registrant to describe the board's oversight of cybersecurity risk • Requires registrant to describe management's role in assessing and managing cybersecurity-related risks
Director cybersecurity expertise (Reg. S-K Item 407(j))	10-K, Proxy Statement	• Requires registrant to disclose the name of any director(s) and relevant details with respect to any directors with expertise in cybersecurity • Such determination does not impose on such director any additional duties, obligations or liability, nor does it affect the duties obligations or liability of any other director

Summary of Proposed Disclosure Requirements

Privacy+ Security Forum

1. Reporting Incidents
    1. Report “material cybersecurity incidents” to the SEC within 4 days
    2. Report non-material incidents that, when combined with other incidents, become material “in the aggregate”
    3. Provide updates on prior incidents in periodic SEC disclosures
2. Reporting about company’s Cyber Posture
    1. Describe company’s cybersecurity risk management system
    2. Describe the Board’s oversight of cybersecurity risk
    3. Disclose the cybersecurity expertise of the Board members

Mandatory material cybersecurity incident reporting

Privacy+ Security Forum

Cooley

LEWIS BRISBOIS

Form 8-K: Report material cybersecurity incidents

Privacy+ Security Forum

- Report **cybersecurity incident** within 4 business days of company's determination that the incident is **material**
- "Cybersecurity incident":
  1. unauthorized occurrence on (or conducted through) company's information systems
  2. that jeopardizes the confidentiality, integrity, or availability of
  3. information systems or any information residing on them
- "Material":
  - substantial likelihood that a reasonable investor would consider information important in making an investment decision or
  - if the information would have significantly altered the "total mix" of information made available
- Cannot delay reporting due to ongoing internal or external investigation (but reporting triggered only on materiality determination)
- Proposed instruction for this requirement that would provide that a company "shall make a materiality determination regarding a cybersecurity incident as soon as reasonably practicable after discovery of the incident"

Form 8-K: Report material cybersecurity incidents (cont'd)

Privacy+ Security Forum

- Disclose details in Form 8-K report (if known):
  1. When the incident was discovered and whether it is ongoing
  2. A brief description of the nature and scope of the incident
  3. Whether any data was stolen, altered, accessed, or used for any other unauthorized purpose
  4. The effect of the incident on the company's operations
  5. Whether the company has remediated or is currently remediating the incident
- Not required to reveal information that would affect incident response or reveal vulnerabilities

Forms 10-Q and 10-K: Provide updates

Privacy+ Security Forum

- Provide material updates to previously disclosed incidents
- Disclose when a series of individually immaterial cybersecurity incidents become material in the aggregate

Reporting about company's Cyber Posture

Privacy+ Security Forum

Cooley

LEWIS BRISBOIS

Form 10-K: Four types of disclosures

Privacy+ Security Forum

1. Company's policies and procedures to identify and manage cybersecurity risks
2. Management's role and expertise in managing cybersecurity risk, policies, and procedures and implementing related policies, procedures, and strategies
3. Board of directors' oversight of cybersecurity risk
4. Board of directors' cybersecurity expertise

Policies and procedures

Form 10-K: Four types of disclosures

Privacy+ Security Forum

1. Company's policies and procedures to identify and manage cybersecurity risks
2. Management's role and expertise in managing cybersecurity risk, policies, and procedures and implementing related policies, procedures, and strategies
3. Board of directors' oversight of cybersecurity risk
4. Board of directors' cybersecurity expertise

Risk management system Operational considerations

Privacy+ Security Forum

- Evaluate company's preparation for security incidents, including whether it has an incident response plan and can use it
- Assess company's ability to detect, investigate, and remediate incidents, including its engagement of forensic firms and outside counsel, and reliance on attorney-client privilege and work-product doctrine
- Review company's ability to analyze for reporting materiality within timeframe specified by proposed rules
- Review company's ability to make disclosures while responding to an incident
- Determine company's involvement of senior management and board

Policies and procedures

Privacy+ Security Forum

- Must disclose any policies and procedures the company has to identify and manage cybersecurity risks and threats, including:
  - Operational risk
  - IP theft
  - Fraud and extortion
  - Harm to employees or customers
  - Violation of privacy laws
  - Other litigation and legal risk
  - Reputational risk

Policies and procedures (cont'd)

Privacy+ Security Forum

- Disclose, as applicable, whether:
  - Company has cybersecurity risk assessment program (and if so, describe)
  - Company engages third parties in connection with risk assessment program
  - Company has a vendor management program (and if so, describe)
  - Company undertakes activities to plan for and respond to cybersecurity incidents (and if so, describe)
  - Company has business continuity, contingency, and recovery plans for cybersecurity incident
  - Previous cybersecurity incidents informed changes to company's governance, policies and procedures, or technologies
  - Cybersecurity-related risks have affected, or are likely to affect, company's strategy, business model, results of operations, or financial condition (and if so, how)
  - Cybersecurity risks are considered as part of company's business strategy, financial planning, and capital allocation (and if so, how)

Operational considerations for company

Privacy+ Security Forum

- Determine cybersecurity risk profile in light of products and services offered, intellectual property, likelihood of government investigation, harm to customers, and importance of reputation to business
- Evaluate technology used and types of data collected
- Evaluate roles of third parties in risk profile and sufficiency of vendor management program
- Assess delineated policies and procedures against business need, industry practice, and practice of peers
- Analyze cost v. benefit of policies and procedures
- Inventory policies and procedures maintained by company and determine disclosure propriety

Management's responsibilities

Form 10-K: Four types of disclosures

Privacy+ Security Forum

1. Company's policies and procedures to identify and manage cybersecurity risks
2. Management's role and expertise in managing cybersecurity risk, policies, and procedures and implementing related policies, procedures, and strategies
3. Board of directors' oversight of cybersecurity risk
4. Board of directors' cybersecurity expertise

Management's responsibilities

Privacy+ Security Forum

- Describe management's role in managing cybersecurity risk and implementing cybersecurity policies and procedures, including:
  - Which management positions or committees are responsible for managing risk, and the relevant expertise of the individuals or committee
  - Whether company has appointed a CISO or similar role, the relevant expertise of the individual, and to whom they report at the company
  - The process by which management is informed of and monitors company's incident preparation and incident response
  - Whether and how frequently management reports to the board on cybersecurity risk

Operational considerations for management

Privacy+ Security Forum

- Determine stakeholders at company responsible for managing risk, and whether they are individuals or committees
- Analyze whether company should appoint a CISO or similar role, depending on information handled by company, overall cybersecurity risk of company, and practice of industry and peers
- Determine management's role in cybersecurity matters, including incident response
- Assess management's reports to board

Board’s responsibilities

Form 10-K: Four types of disclosures

Privacy+ Security Forum

1. Company's policies and procedures to identify and manage cybersecurity risks
2. Management's role and expertise in managing cybersecurity risk, policies, and procedures and implementing related policies, procedures, and strategies
3. Board of directors' oversight of cybersecurity risk
4. Board of directors' cybersecurity expertise

Board's responsibilities

Privacy+ Security Forum

- Describe the board's oversight of cybersecurity risk, including as applicable:
  - Whether the full board, a committee, and/or specific directors are responsible for oversight
  - How the board is informed of cybersecurity risks
  - How frequently the board discusses cybersecurity risks
  - Whether and how the board considers cybersecurity risks as part of company's business strategy, risk management, and financial oversight

Operational considerations for board

Privacy+ Security Forum

- Corporate directors and officers owe specific "fiduciary" duties to company and its stockholders:
  - **Duty of Loyalty** – placing the interests of the company first
  - **Duty of Care** – acting diligently and competently
  - **Duty of Candor** – communicating honestly and fully with stockholders and other directors
  - **Duty of Confidentiality** – protecting boardroom deliberations and company confidential information from disclosure to outsiders

- A director shall discharge his/her duties:
  - *In good faith* – act honestly
  - *With care* – be diligent and deliberate
  - *Like an ordinary person in a like position* – use common sense and practical wisdom
  - *Would exercise under similar circumstances* – context matters
  - *In a manner he reasonably believes* – analyze rationally
  - *To be in the best interests of the corporation* – allegiance to the corporation

Operational considerations for board

Privacy+ Security Forum

- Understand and stay current on the threat landscape and regulatory developments
- Understand the company's measures to address threats and incidents
  - Audit / risk committees, and boards of directors in general, play a significant strategic role in overseeing the risk management activities of the company and monitoring management's policies and procedures
  - Review the company's security and incident response policies to ensure they incorporate required elements and best practices
- Understand when and how incidents will be reported to the board, and the thresholds for reporting up to the board

Operational considerations for board

Privacy+ Security Forum

- Assess the adequacy of policies and resources for cyber incident preparedness and risk mitigation
- Document the committee's / board's review of policies and its role in the oversight of the cyber and incident response preparedness program
- Ensure appropriate training and education within the company and to board members
    - Identify leads within the committee / board on cybersecurity issues and ensure appropriate periodic trainings for the committee (and board, if appropriate) on cybersecurity issues and regulatory requirements
- Ensure that the board is satisfied with the accuracy of (and absence of material omissions in) SEC filings as they relate to cybersecurity risks
- Continue the "tone from the top" on cybersecurity preparedness

Operational considerations for board

Privacy+ Security Forum

- Assign responsible board members with appropriate expertise for oversight (e.g., risk committee or separate subcommittee) with regular updates for the entire board (e.g., annually)
- Assigned board members should receive periodic (e.g., quarterly) updates from management and/or outside experts on recent incidents, trends, vulnerabilities and risk predictions
- Ensure direct reporting line from the InfoSec lead (e.g., CISO) to the board or a committee
- Board should continue to receive regular updates (e.g., quarterly) from management on, and assess the quality / quantity of:
    - cybersecurity initiatives, investments, assessment/testing outcomes, and training;
    - incidents, vulnerabilities, and remediation/strengthening activities; and
    - overall security enhancement roadmap
- Review and ensure satisfaction with SEC filing statements on cybersecurity risks and incidents
- Identify and ensure periodic (e.g., annual) testing against key performance indicators / audit criteria to review the company's cybersecurity risks, defenses, and response processes and benchmark against competitors and industry / regulatory standards

Form 10-K: Four types of disclosures

Privacy+ Security Forum

1. Company's policies and procedures to identify and manage cybersecurity risks
2. Management's role and expertise in managing cybersecurity risk, policies, and procedures and implementing related policies, procedures, and strategies
3. Board of directors' oversight of cybersecurity risk
4. Board of directors' cybersecurity expertise

Board's cybersecurity expertise

Privacy+ Security Forum

- Disclose the names of any directors with cybersecurity expertise (and if so, describe)
- Factors to determine whether a director has "expertise" include:
  - Prior work experience in cybersecurity
  - A certification or degree in cybersecurity
  - Knowledge, skills, or other background in cybersecurity

Operational considerations for board

Privacy+ Security Forum

- Evaluate cybersecurity risk of company and appoint members of the board with appropriate level of cybersecurity expertise
- Consider board composition of peers with respect to cybersecurity expertise
- Determine board's role in cybersecurity matters, including incident response

References

References

- SEC's 2011 interpretative guidance: link
- SEC's 2018 interpretative guidance: link
- SEC's proposed rules: link
- Cooley's summary of proposed SEC rules (March 2022): link
- Cooley's commentary on comments to proposed SEC rules (July 2022): link
- Cooley's cyber/data/privacy blog (link) and public companies blog (link)

Questions & Contacts

Privacy+ Security Forum

Randy V. Sabett, J.D., CISSP
Special Counsel
Cooley LLP
+1 202 728 7090
rsabett@cooley.com

Kamran Salour
Data Privacy & Cybersecurity Attorney
Lewis Brisbois
Kamran.Salour@lewisbrisbois.com
714.966.3184