March 1, 2018

Cybersecurity Governance: *Questions Boards Should Ask Before It's Too Late … and GCs Should Be Prepared to Answer*

Alan Charles Raul

araul@sidley.com

SIDLEY

TALENT. TEAMWORK. RESULTS.

SEC Issues New Guidance On Cybersecurity Disclosure (2/18)

- Commission (not staff) supplements Corp. Fin.'s 2011 guidance on cyber risk
  - Published in Federal Register as "interpretative guidance," not regulation
  - Signals possible enforcement perspectives against public companies whose disclosures or cybersecurity "disclosure controls and procedures" are inadequate
- Newly expanded expectations:
  - Enhance cyber disclosure process: "controls and procedures" must be sufficient to allow CEO and CFO to make required certifications of effectiveness regarding cyber disclosure
    - Companies that support CEO and CFO certifications regarding effectiveness of disclosure controls and procedures with subcertifications by direct reports should consider how these subcertifications will need to be revised and expanded
  - Provide for open communications between technical experts and disclosure advisors
  - Implement insider trading policies to prevent trading on non-public cyber information
- Guidance specifies that controls and procedures should:
  - Enable companies to identify cybersecurity risks and incidents
  - Assess and analyze impact on company's business (considering non-financial factors)
  - Evaluate significance associated with such risks and incidents
  - Make timely disclosures regarding such risks and incidents

Cyber Risk Factors

- Guidance suggests considering these factors when evaluating cyber disclosure:
  - Occurrence, frequency, and severity of prior cybersecurity incidents
  - Probability and potential magnitude of cybersecurity incidents
  - Adequacy of preventative actions taken to reduce cybersecurity risks and costs
  - Aspects of business and operations that give rise to material cybersecurity risks (including industry-specific risks and third-party supplier/service provider risks)
  - Costs associated with maintaining cybersecurity protections, cyber insurance, etc.
  - Potential for reputational harm
  - Loss of IP, competitive advantage, supplier or customer relationships; impacts on products or services
  - Existing or pending laws and regulations that may affect cyber requirements and costs
  - Litigation, regulatory investigation, and remediation costs
- Possible duty to correct or update prior cyber disclosures
- Time needed for internal investigation and cooperation with law enforcement is not a basis to avoid disclosures
  - SEC acknowledges some time is necessary to discern and understand implications

Regulation FD and Selective Disclosure

- Companies should be sensitive to protect against selective disclosure of material information in violation of Regulation FD
- Companies should not selectively disclose material, nonpublic information regarding cybersecurity incidents to Regulation FD enumerated persons before making public disclosure
  - SEC expects that company policies and procedures would address this risk
  - FD persons include: securities market professionals, like brokers, dealers, advisers, fund managers, analysts, shareholders for whom it is reasonably foreseeable they might trade
- Because companies must disclose all material, nonpublic information regarding cybersecurity, net result may be filing a Form 8-K for *material* breaches where notice is provided to affected individuals
  - Otherwise, there could be arguable selective disclosure
- Materiality of breach is very fact-dependent and Form 8-K will not be required for all cybersecurity breaches
  - However, new Guidance may tend to increase amount of public disclosure following material incidents

Board Risk Oversight

- Regulation S-K and Schedule 14A require a company to disclose extent of its board of directors' risk oversight role
  - How board administers its oversight function
  - Board's leadership structure
- To extent cybersecurity risks are material, company should disclose board's oversight of cybersecurity risks
  - Investors should be able to assess how board is discharging its risk oversight responsibility
- SEC notes importance of making disclosures regarding:
  - Company's cybersecurity risk management program
  - How board of directors engages with management on cybersecurity issues

Suggestions for Boards and GCs

- Ensure Board/Audit Committee cybersecurity charter and responsibility is clearly articulated
- Require presentation and maintenance of systematic documentation and data
- Conduct risk assessment/maturity assessments
- Demand explanations of business/security investment trade-offs
- Invest in threat intelligence and understanding of attacker motivation
- Don’t just focus on PII risks; dig into potential operational impacts, business risks, and reputational or compliance implications (focus on SEC factors)
- Escalation protocols are key; develop rigorously and follow scrupulously; develop workable criteria for reporting incidents to Board/CEO
- Formalize process to document fact-finding investigation, systematic analysis, and decisions made
- Rigorous inquiry is necessary and helpful even (or especially) if problems are uncovered
- Adopt skeptical perspective and insist on probing questions and follow-up
- Coordinate internal knowledge sharing and organize decision-making councils; avoid excessive internal compartmentalization and secrecy
- If outside experts are not involved, determine whether that judgment is appropriate
- Legal quarterbacking is critical
- Consider conducting pre-incident “Cybersecurity Legal Governance Assessment”

Cybersecurity Legal Governance Assessment

- Objectives: Enable Board, CEO and GC to address company's cybersecurity governance, legal posture and defensibility on cyber risks; obtain internally focused due diligence and legal advice to help detect, prevent and defend against significant compliance problems, regulatory investigations and foreseeable claims; prepare to manage potential major cyber crises
- Justification: Discharge requisite oversight and fiduciary obligations; position company leadership to demonstrate preparedness and command over the relevant factors before a cyber crisis occurs
- Confidentiality: To support possible invocation of attorney-client privilege and work product confidentiality, the assessment should be primarily or substantially for the purpose of providing legal advice regarding compliance and defense of future claims (note: applicability of legal confidentiality will depend on specific circumstances)
- Cybersecurity Issues to Probe:
- Understand responsibilities, organization, spending, reporting and accountability for cybersecurity program
- Review information security and incident response programs
- Understand and decide whether and how company applies NIST Cybersecurity Framework

Cybersecurity Legal Governance Assessment – cont'd

- Understand whether company applies or is subject to any other external standards (e.g., ISO, PCI, FFIEC, etc.)
- Review existing risk assessments, and ongoing risk assessment process
- Review cyber asset management process for identifying critical systems and information (i.e., "crown jewels"), and setting priorities for commensurate safeguards
- Understand import of existing threat intelligence reports
- Review insider threat program and experience
- Review results of existing penetration tests, and ongoing process
- Understand process and review existing internal audit reports
- Understand process and review external audit reports
- Review company's history of incidents, handling of incident response and legal claims (and analogous situations for relevant peers)
- Review processes to identify, track, log and resolve "red flags"
- Probe and understand any current significant pending or unresolved red flags

Cybersecurity Legal Governance Assessment – cont'd

- Review and understand key third-party and service provider relationships
- Review oversight, monitoring and diligence regarding third-parties/service providers
- Evaluate clearance process for company's SEC cybersecurity risk factor language
- Review any communications with company's outside auditor regarding cyber
- Review process for considering cybersecurity in significant M&A transactions
- Understand and evaluate company's cyber compliance culture
- Receive comparison/benchmarking information regarding peers
- Review, evaluate and assure adequacy of budget, staffing, resources and support from management
- Judge whether Board and C-Suite are sufficiently involved
- Understand significant perceived risks, weaknesses, significant "unsuccessful" attacks, and serious fears of InfoSec team
- Consider process or organizational refinements to enhance company's cyber compliance and defense posture

Alan Charles Raul

Partner

Washington, D.C.
+1 202 736 8477
+1 202 736 8711 FAX
araul@sidley.com

PRACTICES

- Privacy and Cybersecurity
- Supreme Court and Appellate
- White Collar: Government Litigation & Investigations
- Government Strategies

INDUSTRY

- Financial Services
- Technology
- Media and Entertainment
- Life Sciences

ADMISSIONS & CERTIFICATIONS

- U.S. Supreme Court
- U.S. Court of Appeals, 2d Circuit
- U.S. Court of Appeals, D.C. Circuit
- U.S. District Court, S.D. of New York
- U.S. District Court, District of Columbia
- Other federal courts
- District of Columbia
- New York

ALAN RAUL is the founder and leader of Sidley's highly ranked Privacy and Cybersecurity practice. He represents companies on federal, state and international privacy and cybersecurity issues, including global data protection and compliance programs, data breaches, consumer protection issues and Internet law. Alan advises companies regarding their cybersecurity and information governance and preparedness, and helps them address crisis management for data security incidents. Alan's practice involves litigation and counseling regarding consumer class actions and investigations, enforcement actions and policy development by the FTC, State Attorneys General, SEC, Department of Justice and other government agencies.

Most recently, Alan has represented a special cybersecurity review committee of the Board of Directors of a major tech company in connection with its independent investigation of the company's handling of significant data breaches.

Alan provides clients with perspective gained from extensive government service. He previously served as Vice Chairman of the White House Privacy and Civil Liberties Oversight Board, General Counsel of the Office of Management and Budget, General Counsel of the U.S. Department of Agriculture, and Associate Counsel to the President.

Alan serves as a member of the Data Security, Privacy, and Intellectual Property Litigation Advisory Committee of the U.S. Chamber Litigation Center (affiliated with the U.S. Chamber of Commerce). He also serves *ex officio* on the American Bar Association's Cybersecurity Legal Task Force by past appointment of the ABA President, and as a member of the Practicing Law Institute's (PLI) Privacy Law Advisors Group.

Alan is a member of the governing Board of Directors of the Future of Privacy Forum. He also serves on the Executive Committee of the Federalist Society's Administrative Law Practice Group. Alan is a frequent author and speaker on privacy, cybersecurity and related issues. He is overall editor and a contributing author of *The Privacy, Data Protection and Cybersecurity Law Review* (Law Business Research Ltd, 4th ed. Dec. 2018).

Alan holds degrees from Harvard College (AB *magna cum laude*), Harvard Kennedy School of Government (MPA), and Yale Law School (JD). He clerked for Judge Malcolm R. Wilkey of the U.S. Court of Appeals for the D.C. Circuit.