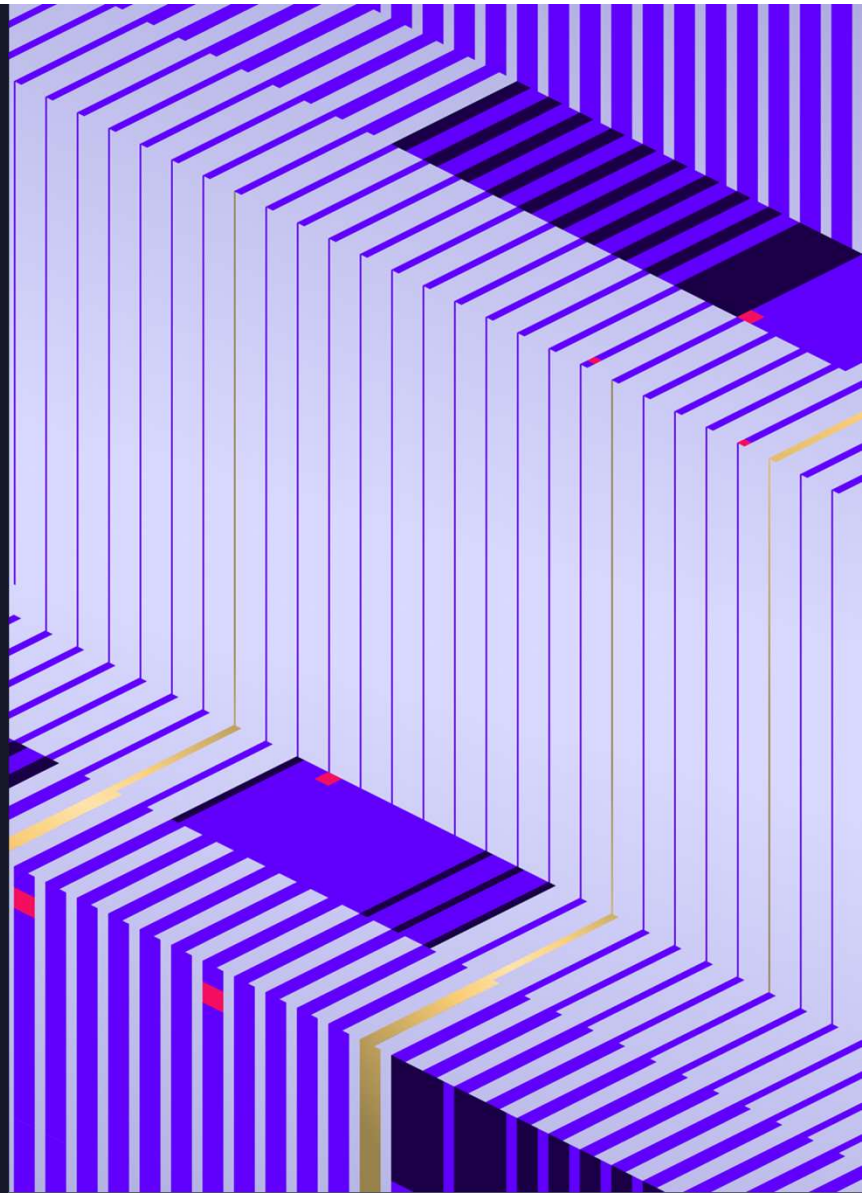
Charleston CyberLaw Forum

January 23, 2025

SentinelOne Secure Tomorrow

CHARLESTON SCHOOL OF LAW

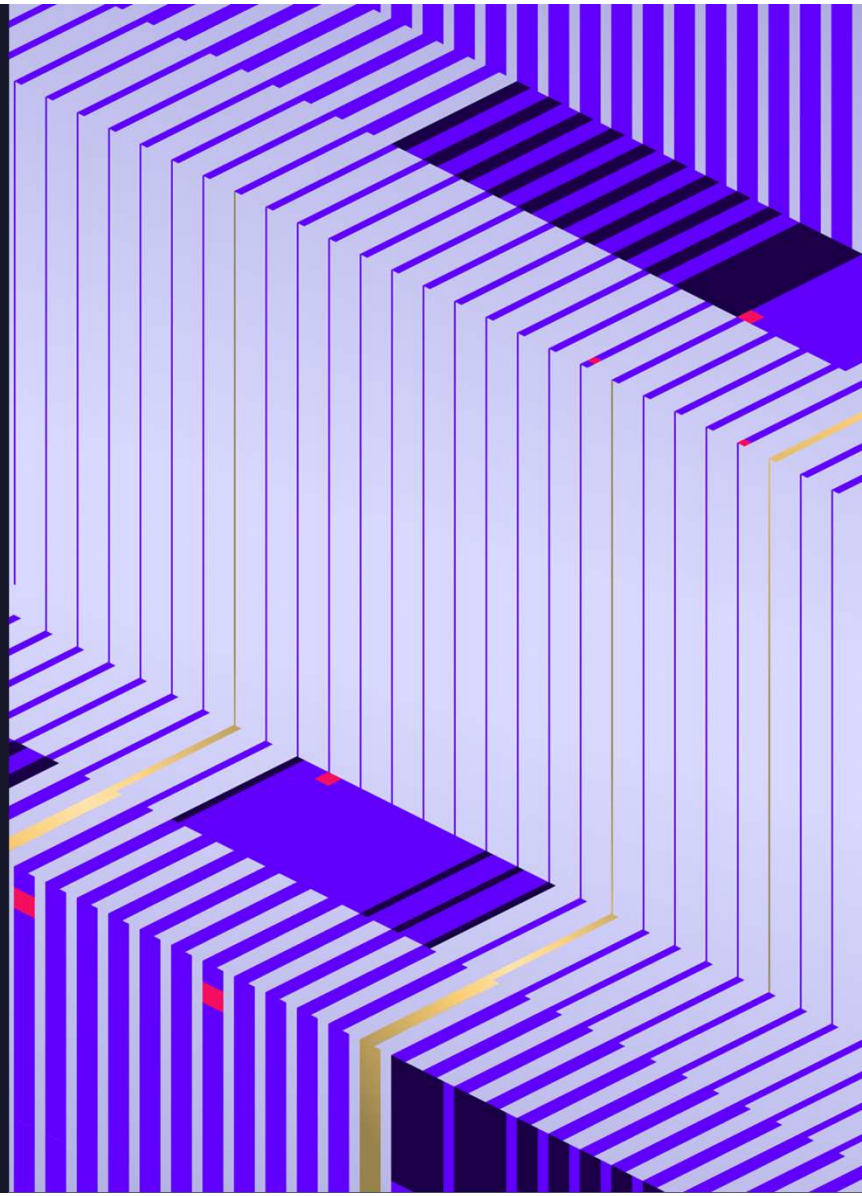


Regulatory: Hot Topics

The CLE materials are sponsored by SentinelOne and Charleston Law School. All CLE materials are prepared by law firms and attorneys as noted in the materials, and do not offer any specific legal advice or guidance.

SentinelOne
Secure Tomorrow

CHARLESTON
SCHOOL OF LAW



Presenters

Evan Wolff

Co-Chair Privacy & Security

Crowell

Randy Sabett

Special Counsel

Cooley

Dave Lashway

Partner, Privacy & Security

Sidley

Rob Knake

Principal

Orkestral

SentinelOne CHARLESTON SCHOOL OF LAW

Discussion Outline

- **General regulatory trends**
  - What's in store for 2025?
- **Specific issues:**
  - CMMC – regs and certification
  - SEC – cyber rules
  - CIRCIA…or CIR 'see yah'?
  - NIS2
  - FCC – Salt Typhoon
- **Other matters to note:**
  - Harmonization (DHS/CISA/CSRB/etc.)
  - FAR/DFARS – contracts and CUI
  - TSA – rail and pipeline cyber proposals
- **Path forward:**
  - Overcoming challenges and transitions

SentinelOne

Evan Wolff

Co-Chair Privacy & Security, Crowell

Crowell

Evan D. Wolff is a partner in Crowell & Moring's Washington, D.C. office, where he is co-chair of the firm's Chambers USA-ranked Privacy & Cybersecurity Group and a member of the Government Contracts Group. Evan has a national reputation for his deep technical background and understanding of complex cybersecurity legal and policy issues. Calling upon his experiences as a scientist, program manager, and lawyer, Evan takes an innovative approach to developing blended legal, technical, and governance mechanisms to prepare companies with rapid and comprehensive responses to rapidly evolving cybersecurity risks and threats. Evan has conducted training and incident simulations, developed response plans, led privileged investigations, and advised on hundreds of data breaches where he works closely with forensic investigators. Evan also counsels businesses on both domestic and international privacy compliance matters, including the EU General Data Protection Regulation (GDPR), and the California Consumer Privacy Act (CCPA). He is also a Registered Practitioner under the Cybersecurity Maturity Model Certification (CMMC) framework.

Randy Sabett

Special Counsel, Cooley

Cooley

Randy V. Sabett, CISSP, counsels clients on a wide range of cutting-edge cybersecurity, privacy, IoT, IT licensing and intellectual property issues. Randy helps clients develop strategies to protect their information, including advising companies on developing and maintaining appropriate internal controls to meet privacy and cybersecurity requirements. He also drafts and negotiates a wide variety of technology transaction agreements. Having previously served as an in-house counsel to a Silicon Valley startup, Randy employs a pragmatic approach when structuring and negotiating such agreements. He has also counseled numerous clients on a variety of data breach scenarios, including running incident response for major commercial retailers, large financial institutions, on-line service providers and healthcare organizations.

Dave Lashway

Partner, Privacy & Security, Sidley

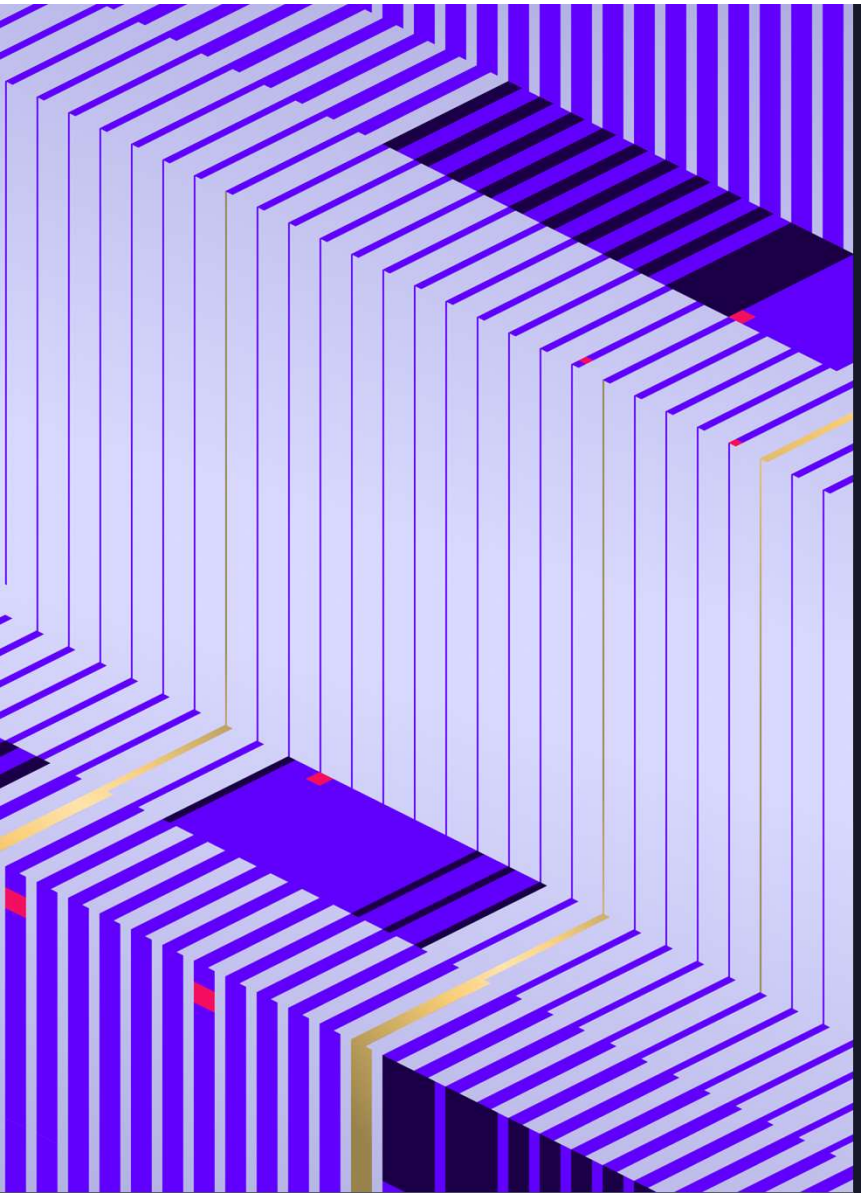
SIDLEY

David Lashway is co-chair of Sidley's highly ranked global Privacy and Cybersecurity practice and a member of the firm's top ranked Crisis Management and Strategic Response team. He is acknowledged as one of the leading lawyers for crisis management, cybersecurity, data security incidents, misinformation, trade secret theft, and related investigation matters. He has advised private and public organizations on significant and material cybersecurity incidents across almost every critical infrastructure sector, including financial services, energy, manufacturing, technology, water, defense, municipal government, retail, transportation, and hospitality industries. He has significant experience in addressing election security and misinformation-related issues, and was deeply involved in the investigations into the 2016 and 2020 actions targeting various U.S. political parties. He has served as the lead lawyer advising on the legal response to operationally impactful malware for a number of Fortune 500 entities, and led the incident response, associated investigations and litigations for several companies impacted by the NotPetya malware incident. He routinely leads responses to ransomware-related matters.

Rob Knake

Principal, Orkestral

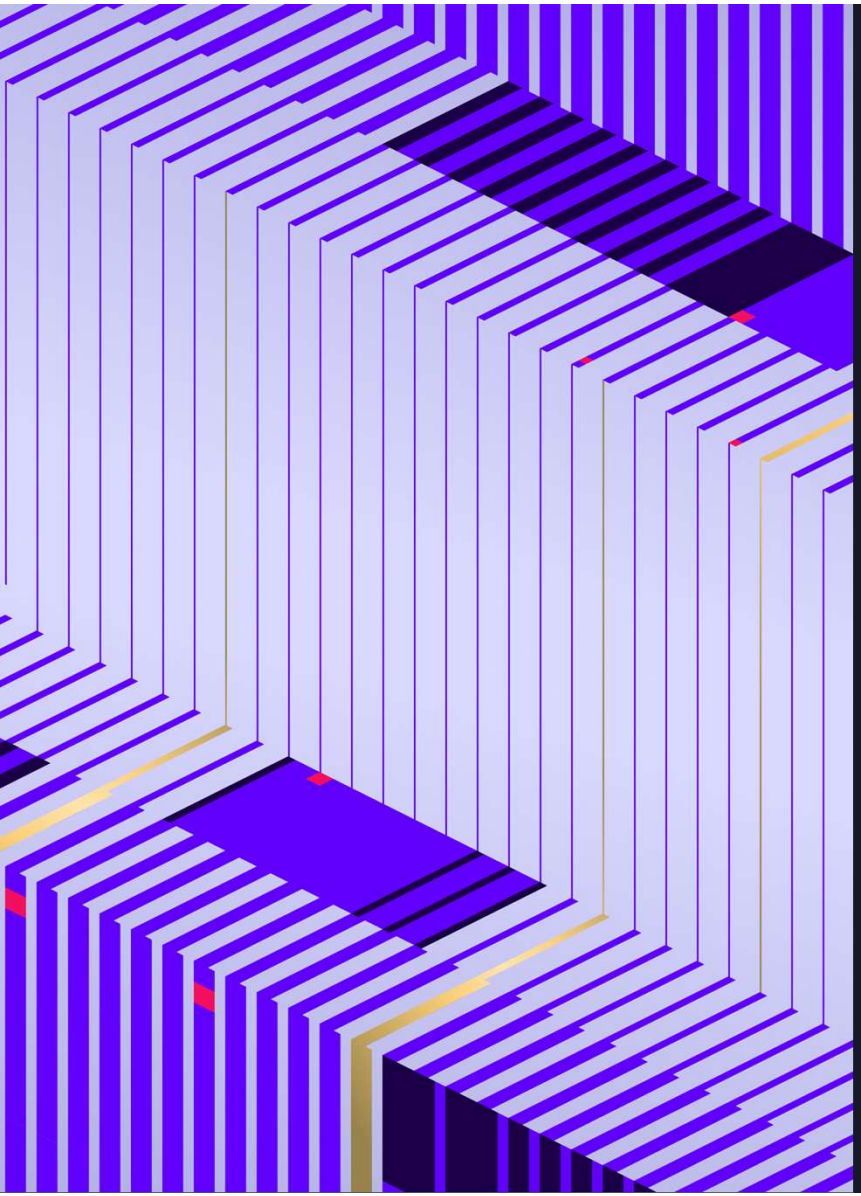
Rob Knake is a principal at Orkestrel, a cybersecurity consultancy and a widely recognized expert and government leader on cybersecurity. Rob served as the first Deputy National Cyber Director in the newly created Office of the National Cyber Director at the White House from 2022 to 2023. In that role, he helped to standup the organization and led the development of the National Cybersecurity Strategy. He also led the development of the first ever cybersecurity budget priorities for the Federal government among other initiatives. In previous government service, Rob served from 2011 to 2015 as Director for Cybersecurity Policy at the National Security Council. In the private sector, Rob has advised Fortune 500 companies, startups, and private equity firms on cybersecurity practices, incident response, and strategy as well as mergers and acquisition. In the think tank community, Rob has been a Senior Fellow at the Council on Foreign Relations, a Cyber Fellow at Harvard's Belfer Center, a Senior Research Scientist at Northeastern University and has taught at Georgetown University. He has co-authored two books on cybersecurity with Richard Clarke, *Cyber War: The Next Threat to National Security* and *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats.* He has testified before Congress four times.



SentinelOne
Secure Tomorrow

Thank You

Sentinelone.com



SentinelOne
Secure Tomorrow

Appendix

Sentinelone.com

The Board's Duty of Oversight

Cooley

Delineating the Board's Role

- Board's fiduciary duties require that directors engage in active, informed ***oversight*** of the management of key corporate risks
- Court decisions do not require boards to engage in independent fact-finding efforts, but ***boards should consider what procedures are in place to ensure they are receiving sufficient factual information about prioritized risk areas on a regular basis***
- Directors may rely on reports and advice of appropriate officers, employees, counsel and advisors

Cybersecurity Oversight Landscape

- As technology becomes increasingly integral to almost every part of an organization's operations, the cybersecurity risks confronting corporations grow
- Cybersecurity risks to companies' bottom lines can be direct (through class actions, fines and investigation costs) and indirect (through reputation damage that can threaten revenue and market share)
- The exposure extends to companies' boards, which are increasingly liable for cybersecurity as part of their fiduciary responsibilities
  - Per the SEC: "effective cyber security programs start with the right tone at the top, with senior leaders who are committed to improving their organization's cyber posture through working with others to understand, prioritize, communicate, and mitigate cyber security risks"
  - The FTC recently emphasized the key role corporate boards play in a successful cybersecurity program
- Given the importance of cybersecurity risks for pretty much every organization, companies are increasingly seeking board candidates with targeted IT/cybersecurity expertise

Responsibilities in the Cybersecurity Context

- Directors should ensure that they are regularly and adequately informed regarding, and satisfied with, the company's cybersecurity risk management and incident-response preparedness and plan (***including the procedures to discover breaches and notify the disclosure committee, management and board when a material breach is discovered***)
- Directors should also ensure that they are satisfied with the accuracy of (and absence of material omissions in) SEC filings
- Consider whether Board or relevant committee has adequate knowledge and understanding to provide oversight (taking into account the ability to rely on advisors)

Responsibilities in the Cybersecurity Context (cont.)

- During a material breach situation, directors should receive periodic reports from management regarding:
  - Learnings regarding the breach, which evolve over time
  - Execution of incident response plan – satisfy themselves it is being executed
  - But let management execute the plan – fast timeline, highly technical, need for decisive action, company needs to speak with “one voice”
- After a material breach, directors should receive a debrief on what happened, success of incident response plan, how gaps or continuing consequences are being addressed
- “Material” should be considered qualitatively as well as quantitatively

Background and overview of SEC cybersecurity rule

Cooley

Background on cybersecurity disclosure requirements

Lessons from recent enforcement actions

- **Incident response and vulnerability policies to ensure senior management analysis.** Companies must have adequate disclosure controls and procedures in place to allow for the timely informing of senior decision-makers so that disclosure decisions concerning cybersecurity incidents and vulnerabilities are made with knowledge of all pertinent facts
- **SEC's views on disclosure.**
  - A hypothetical risk factor regarding cybersecurity intrusions may not be sufficient if an actual event or vulnerability has been found and is deemed disclosable
  - When companies speak about cybersecurity incidents, they must carefully choose their words and appropriately disclose relevant details concerning the incident (i.e., avoid material omissions)
  - As information regarding a cybersecurity incident evolves, prior disclosures may need to be updated

High-level summary of disclosure requirements

Disclosure item	SEC form(s)	Summary of disclosures
Material cybersecurity incidents	8-K	• Disclose material cybersecurity incident within four business days of determining materiality (subject to narrow national security and public safety delay exception) • Describe the *material* aspects of the incident's (i) nature, scope and timing; and (ii) impact, or reasonably likely impact, on the company, including its financial condition and results of operations
Risk management and strategy	10-K	• Describe processes for the assessment, identification and management of material risks from cybersecurity threats • Describe whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected, or are reasonably likely to materially affect, the company's business strategy, results of operations or financial condition
Governance	10-K	• Describe management's role in assessing and managing material risks from cybersecurity threats • Board's oversight of risks from cybersecurity threats

Cybersecurity incident reporting obligations

Cooley

Key terms

- "**Cybersecurity incident**": an *unauthorized occurrence*, or a *series of related unauthorized occurrences*, on or conducted through a *company's information systems* that jeopardizes the confidentiality, integrity, or availability of a company's information systems or any information residing therein.
  - "Paper breaches"
  - Accidental / inadvertent disclosures
  - Unexploited vulnerabilities?
- "**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
  - SEC 2011 and 2018 cyber guidance discusses materiality for purposes of financial reporting
- "**Cybersecurity threat**": any potential unauthorized occurrence on or conducted through a company's information systems that may result in adverse effects on the confidentiality, integrity or availability of a company's information systems or any information residing therein.

Form 8-K: Report material cybersecurity incidents

- Report **cybersecurity incident** within 4 business days of company's determination that the incident is "**material**"
- Cannot delay reporting due to ongoing internal or external investigation (but reporting deadline triggered only on materiality determination)
  - SEC's clarifying comments**: *The registrant will develop information after discovery until it is sufficient to facilitate a materiality analysis*"**
- Instruction for this requirement is that companies make their materiality determinations "without unreasonable delay."

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

Disclose in Form 8-K report (if known):

- The material aspects of the nature, scope and timing of the incident
- The material impact, or reasonably likely material impact on the company, including its financial condition and results of operations

Not required to reveal information that would affect incident response or reveal vulnerabilities

Obligation to update 8-K or other relevant filings when unknown details become known

National security / public safety exception

- Delayed filing of 8-K is permissible where the US attorney general has notified the SEC in writing that the disclosure poses a substantial risk to national security or public safety
- Initial delay of up to 30 days may be extended if US attorney general determines that disclosure continues to pose a substantial risk to national security or public safety up to 120 days
- Beyond these 120 days of potential delay, if the attorney general indicates that further delay is necessary, the SEC will consider additional requests and grant any relief throug an SEC exemptive order
- FBI guidance “in the coming weeks” regarding the intake and evaluation process

SentinelOne

Operational considerations

Undertake an evaluation under legal privilege of the incident response plan and playbooks, vulnerability management program and internal controls for appropriateness in light of rule

Develop ‘playbook’ for establishing attorney-client privilege to protect the sanctity of the decision-making process around reporting

Weave materiality into the incident response plan (potentially a separate playbook)

- Develop criteria / approach for determining materiality in the cyber context, consider pre-established “business impact assessments”
- Consider how “reasonable investigation” time can be built into the materiality determination
- Develop escalation path and appropriate team for materiality determination
- Include accounting team / CFO in the incident response team to help with materiality determinations
- Differentiate between information security “severity ratings” and material business impacts

Operational considerations

Key elements of incident response plans and playbooks:

- Holistic / multi-stakeholder response plan – i.e., not just an IT response plan – that addresses areas of responsibility and enables business impact and materiality determinations
- Escalation procedures – define triggers, paths and reporting lines (including to disclose to those responsible for materiality analysis as well as board/committees of board)
- Addresses more than just personal data incidents – include any incidents that could have a material impact on the company's operations, ability to provide services or products, reputation or customer loss
- Address third-party vendor breaches, including with respect to materiality analysis
- Identifies key vendors for incident response with contact details; consider pre-on boarding
- Addresses communications, including creation of a communications playbook

Training and testing, including potentially penetration tests, vulnerability scanning, tabletop exercises, red/blue team testing, business continuity/disaster recovery (including recovery/restoring from back-ups)

Cybersecurity risk management, strategy and governance disclosures

Cooley

Annual Report disclosures (Item 106 Reg. S-K)

- **Processes.** Describe the company's processes, if any, for assessing, identifying and managing material risks from cybersecurity threats in sufficient detail for a reasonable investor to understand those processes. In providing such disclosure, a company should address, as applicable, the following non-exclusive list of disclosure items:
  - Whether and how the described cybersecurity processes have been integrated into the company's overall risk management system or processes
  - Whether the company engages assessors, consultants, auditors or other third parties in connection with any of these processes
  - Whether the company has processes to oversee and identify material risks from cybersecurity threats associated with its use of any third-party service provider
- **Cyberthreats/risks.** Describe whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the company, including its business strategy, results of operations, or financial condition and if so, how

Annual Report disclosures (Item 106 Reg. S-K) Management governance disclosures

Rule: Describe management's role in assessing and managing material risks from cybersecurity threats, including, but not limited to, disclosure of the following information:

- Whether and which management positions or committees are responsible for assessing and managing these risks, and the relevant expertise of such persons or members in enough detail as necessary to fully describe the nature of the expertise
- The processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation and remediation of cybersecurity incidents
- Whether such persons or committees report information about these risks to the board or a committee or subcommittee of the board

Annual Report disclosures (Item 106 Reg. S-K)
Board governance disclosures

- Rule:
  - Describe the board's oversight of risks from cybersecurity threats
  - If applicable, identify the board committee or subcommittee responsible for this oversight of risks from cybersecurity threats
  - Describe the processes by which the board or this committee is informed about these risks

Annual Report disclosure challenges

- Organizations lacking or maintaining immature “processes for assessing, identifying, and managing material risks”
- Organizations without formal written “processes” for managing material risks
- Identifying gaps/problems with risk management program (explicitly or by omission) that cannot be remediated prior to making disclosures
- Overstating or misstating a company’s security processes (e.g., plaintiffs or regulators alleging “misrepresentations” around security)
- Boiling down disclosures on complex security topics so they can be understood by a “reasonable investor”

Operational considerations

- Undertake legally privileged audit and assessment of current processes for assessing, identifying and managing material risks for alignment with the rules, including:
  - Company's risk profile given its industry, market position, technology used and types of data collected
  - Evaluate roles of third parties in risk profile and sufficiency of vendor management program
  - Assess processes against business need, industry practice, practice of peers and applicable standards and certifications
- Develop action plan under legal privilege for enhancements to risk management program and strategy
- Determine how best to describe the processes and material risks in response to disclosure requirements
- Review existing disclosures relating to cybersecurity (in financial statements, websites, marketing materials, etc.) for any updates and/or inconsistencies

Operational considerations for management

- Determine stakeholders at company responsible for managing risk, and whether they are individuals or committees
- 1
- 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
- 2
- Determine management's role in cybersecurity matters, including incident response
- 3
- Assess management's reporting to board, including frequency, content and involvement in incident response
- 4
- Assess communications, collection of data and response plans with third party service providers
- 5

Operational considerations for company

- Board considerations
  - Should there be a specific cybersecurity subcommittee?
  - Cybersecurity expertise / training / specialist input?

Operational considerations for board

- Discuss with management 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
- Continue the "tone from the top" on cybersecurity preparedness

Operational considerations for board

- Assign responsible board members with appropriate expertise for oversight (e.g., risk committee or separate subcommittee) with regular updates for the entire board
- Assigned board members should receive periodic updates from management and/or outside experts on recent incidents, trends, vulnerabilities and risk predictions
- Ensure direct reporting from the InfoSec lead (e.g., CISO) to the board or a committee
- Board should continue to receive regular updates 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
- Identify and ensure periodic 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

Operational considerations for board

- 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
- Understand when and how incidents will be reported to the board, and the thresholds for reporting up to the board

Cybersecurity Maturity Model Certification (CMMC)

2013 – 2016	*Jan 2020*	*Sept 2020*	*Oct 2021*	*Late 2024*			
Safeguarding CUI DFARS 7012	**CMMC Introduced**	**NIST Basic Assessment**	**DOJ Civil Cyber Fraud Initiative**	**CMMC Active**	**Finish Preparedness**	**C3PAO Assessments**	**Annual Monitoring / Affirmations**

Why Is This Hard?

- Identifying CUI on networks is difficult as it can be everywhere
- Networks are increasing in scale and complexity
- Applying the 110+ security controls requires technical & administrative demands
- Supply chain compliance challenges create systemic risk
- Requires third party assessors
- The legal risk of getting compliance wrong is significant

What is Everyone Doing?

- Scoping CMMC assets
- Conducting privileged compliance assessments
- Interviewing & engaging C3PAOs for audits
- Updating technical controls:
  - MFA, vulnerability management, FIPS cryptography, mobile device management
- Focusing on supply chain

Where Is This Going?

- Phased implementation over 7 years throughout DIB
- NIST SP 800-171, **Revision 3**
- FAR CUI Rule applying requirements governmentwide

SentinelOne