Cooley

SEC Reporting Skills Workshop

David Navetta

Asa Henin

Operationalizing SEC Cybersecurity Disclosure Rule – 2024

attorney advertisement

Agenda

- Quick background
- Incident response challenges and strategy: developing a materiality assessment process for 8-K disclosures
- Developing cyber disclosures for 10-K
- SEC v. Solarwinds – implications and action items
- Conclusion and Q&A

Background on the SEC's cybersecurity rule: developing a materiality assessment process for 8-K disclosures

Cooley

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

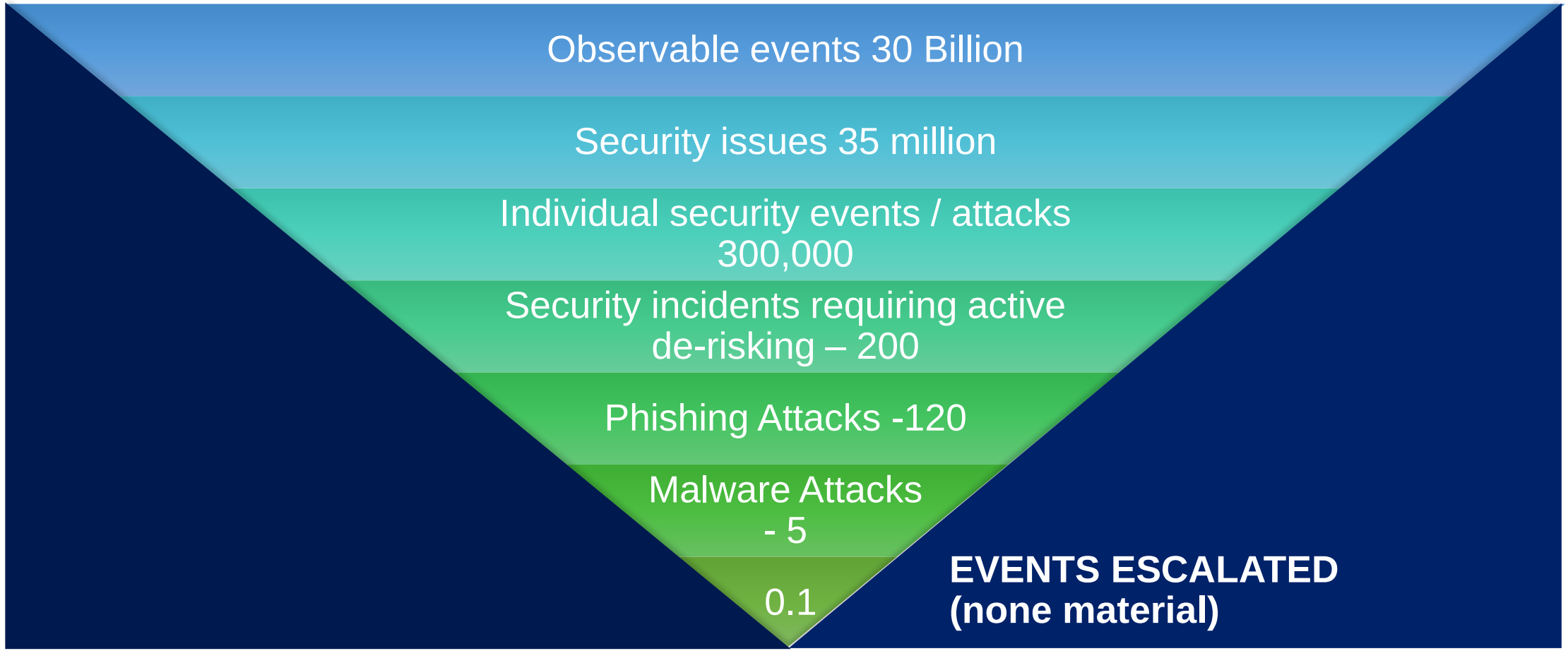
Incident response challenges and strategy

Cooley

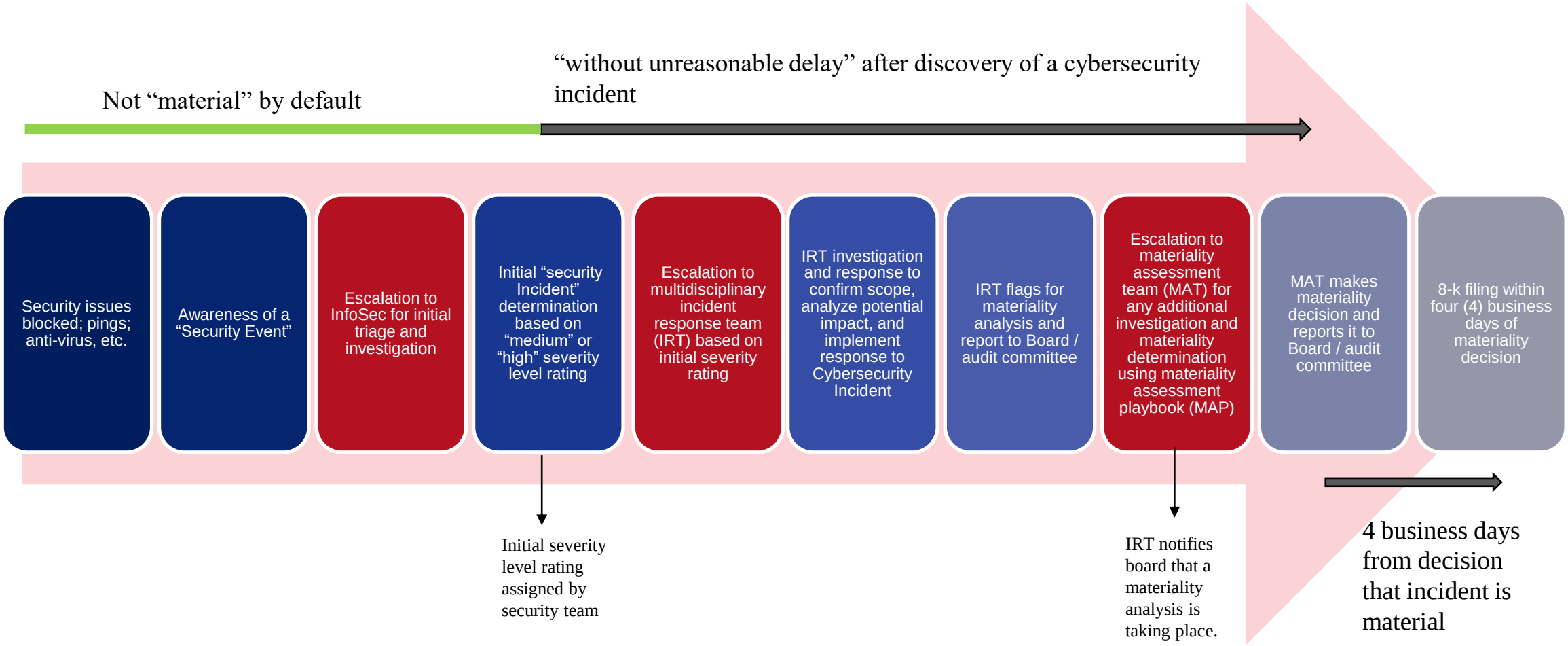
Form 8-K: Report material cybersecurity incidents

- Companies must make their materiality determinations "without unreasonable delay" after discovery of a cybersecurity incident
- Report **cybersecurity incident** within 4 business days of company's determination that the incident is "**material**"
  - Exception: national security / public safety concern approved by the USAG
- 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*"**
- **Required disclosures:**
  - 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

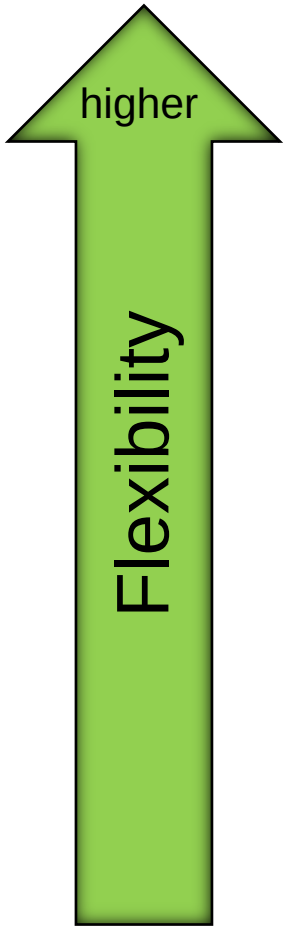
Security incident funnel sample (monthly)



ARE -- 8-K cybersecurity incident escalation and reporting



Operational considerations
Materiality assessment playbook/process ("MAP") options



- High-level playbook based on general factors identified by SEC ("know-it-when-you-see-it")
- Criteria and scenario-based MAP without prescriptive/binary decision points
- Prescriptive / binary MAP ("if/then" approach)

Operational considerations
Criteria / scenario-based materiality assessment

POTNETIAL MATERIAL IMPACTS: Identify potential material impacts that could result from a cybersecurity incident

MATERIALITY CRITERIA: Identify the criteria needed to make a materiality decision for each impact

(quantitative, qualitative, mitigation criteria)

INFORMATION INPUTS: Identify the information needed to analyze the materiality criteria

- **Information about an incident**: what happened, what information systems/data were affected, how were they affected?
- **Information needed to assess business impact:** what do we need to know to determine if a material impact has occurred or is reasonably likely to occur?

REAL-TIME INCIDENT MITIGATION: can the scope of the incident be reduced and can the business impact be mitigated below materiality threshold?

Sample scenario-based MAP (ransomware attack) -- quantitative criteria

Criteria	Information inputs	Response impact mitigation
Quantitative – revenue / income loss	• Revenue / income loss per relevant time increment (e.g. per hour/per day, etc.)	Minimizing down time by shutting down unaffected systems, restoring from backups, or restoring using decryption key obtained by threat actor
Quantitative – ransom demand payment	• Initial / negotiable extortion demand • Threat actor identity and prior history/patterns	Paying the ransom may allow for faster or more complete restoration and recovery of data/systems
Quantitative – costs to respond to incident	• Amounts anticipated costs for: forensics; legal; ransom negotiator; recovery; PR, etc.	Vendor liability / indemnification (if applicable)
Quantitative – data asset loss	• Value of data assets that cannot be recovered	Vendor liability / indemnification (if applicable)
	• Costs necessary to restore or recreate lost data assets	Existence/availability of back-ups or other source material needed to recreate data assets
Quantitative – customer litigation defense judgments / settlements / defense costs	• Impact to customers	Use of BC/DR techniques
	• Existence of a breach of contract	Vendor liability / indemnification (if applicable)
	• Scope of limitations of liability	
	• Defense costs	
	• Litigation viability and history	
Quantitative -- cyber insurance (or other) coverage	• Limitations of liability for insurance • Confirmation of coverage for quantitative criteria	• Aggressive insurance broker • Insurance coverage counsel

Cybersecurity risk management, strategy and governance disclosures

Cooley

Annual Report disclosure summary (Item 106 Reg. S-K)

Risk assessment and management 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.

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.

Management's role. Describe management's role in assessing and managing material risks from cybersecurity threats.

The board's role. Describe the board's oversight of risks from cybersecurity threats.

Key considerations for developing 10-K content

- Accuracy and completeness are paramount
- Proper scoping
- Reconcile against other external security statements
- Avoid temptation to overstate security and/or compliance with standards (this is not a marketing opportunity)
- Balancing act: helpful to investors v. revealing too much
- Cyberthreat reporting requirement vs. risk factors
- “Customized”

SEC v. Solarwinds – implications and impacts

Cooley

Solarwinds allegations

- **Three different sets of disclosures:** (1) financial disclosures/risk factors (S1, S-8 [and by extension 10-K); (2) public statements/marketing materials (the “Security Statement” on its public website); and (3) internal comms: emails, slack messaging, reports, pentest results, etc.
- **The SEC looked at a combination of issues and the failure to report vulnerabilities (individually or collectively) in 10-k risk factors was allegedly materially misleading (by omission)**
  - General statements concerning bad security
  - Failure to implement ‘secure development lifecycle” practices
  - Failure to enforce the use of strong passwords (e.g. failure to comply with its own internal policies)
  - Failure to address remote access issues for years
  - Access control issues for critical systems
  - Backends not resilient
  - Constant losing battle against remediation of vulnerabilities
  - Statement that SW “follows” NIST (where only 40% of the NIST 800-53 controls were “met or partially met[,] leaving 60% completely unmet; also SW had a NIST score of 3, which SW believes is ‘good’)
- **Deficiencies in 8-K** – vulns posed as hypotheticals that could be exploited, when in fact they had been exploited and the Company knew it.

Security representations

- **What you say matters.** The SEC alleged that SolarWinds should have reported its vulnerabilities and security weaknesses even if SolarWinds did not suffer a security breach resulting from them.

- **Security-related statements in many areas are subject to SEC scrutiny.**
  - Financial disclosures/risk factors (e.g., S1, S-8, 10-Q/10-K)
  - Public statements/marketing materials (e.g., the “Security Statement” on SolarWinds’s public website)
  - Internal communications and materials (e.g., emails, Slack messages, security reports including results of pentests)
  - SEC compared the representations made in each context to each other to look for inconsistencies and omissions

Internal communications

- **Reconcile communications regarding security**
  - **Potential sources of 'external statements':** security whitepapers, trust & safety web pages, security and privacy web pages, security-related summaries, developer documents/alerts, marketing materials, blogposts, privacy policies.
  - **Potential sources of 'internal statements':** security assessment reports, penetration test results, security audits by third parties, emails, slack messages, security-related reports to management/boards
- **Security communications training**
  - Build a culture of accurate communications
  - Consider the informality of the forum
  - Focus should be on factual statements, not unsubstantiated / off-the-cuff opinions or inflammatory statements
  - Provide context (e.g. CVSS vuln scoring, heatmaps)
  - Use attorney-client privilege, but beware

The Ten Communication C's

1. **Correct.**
2. **Complete.**
3. **Character.**
4. **Contextualized**
5. **Consistent.**
6. **Corroborate.**
7. **Clear.**
8. **Cooperative.**
9. **Choose your medium.**
10. **Choose your words.**

Key takeaways

- **Connect the dots:** analyze materiality holistically – a combination of security issues may be material where a single issue is not
- **Avoid hypothetical risk factors** if the hypo has already occurred (alleged material omission)
- **Inconsistent reps about security used as evidence of fraud** – not just in financial statements, but on security-related marketing pieces and inside security chatter
- **CISOs at risk.** Consider CISO's reaction to this decision (e.g. D&O insurance, more direct reporting/CYA, etc.)

Q&A

Cooley

Speakers

Dave Navetta
Partner
cyber/data/privacy
+1 720 566 4153
dnavetta@cooley.com

Asa Henin
Special Counsel
Public Companies
+1 858 550 6104
ahenin@cooley.com