ALSTON & BIRD

SEC Cybersecurity Disclosure Rules: Ready or Not, Here They Are

November 8-10, 2023, Privacy + Security Forum, Fall Academy

Speakers

Kate Hanniford

Partner,

Alston & Bird

Katharine Cralle

Partner,

Brunswick Group

Julie Mediamolle

Partner,

Alston & Bird

Agenda

1. Welcome and Introductions
2. Overview of the New Rules
3. Practical Considerations
4. Q&A

Overview of the New Rules

SEC's New Cybersecurity Reporting – Form 8-K

- Report a material cybersecurity incident on Form 8-K within four business days after determining that such incident is material.
- Materiality determination made "without unreasonable delay".
- Need to describe incident's nature, scope, timing and impact (actual or likely) – less granular information than originally proposed.
- Amend the Form 8-K as necessary to provide any information what was unavailable or make corrections if information was found incorrect or misleading.

New Cybersecurity Disclosures in Form 10-K

Process for Assessing and Managing Cybersecurity Risks

- Describe processes for assessing, identifying and managing material risks from cybersecurity threats. Disclosure could include:
  - How 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 such processes.
  - Whether the company has processes to oversee and identify such risks from cybersecurity threats, associated with its use of any third-party service provider.
  - Description of prevention and detection activities and continuity and recovery plans.
  - Description of prior incidents.
  - Whether any cybersecurity risks have materially affected or are reasonably likely to materially affect the company's business strategy, results of operations or financial conditions.

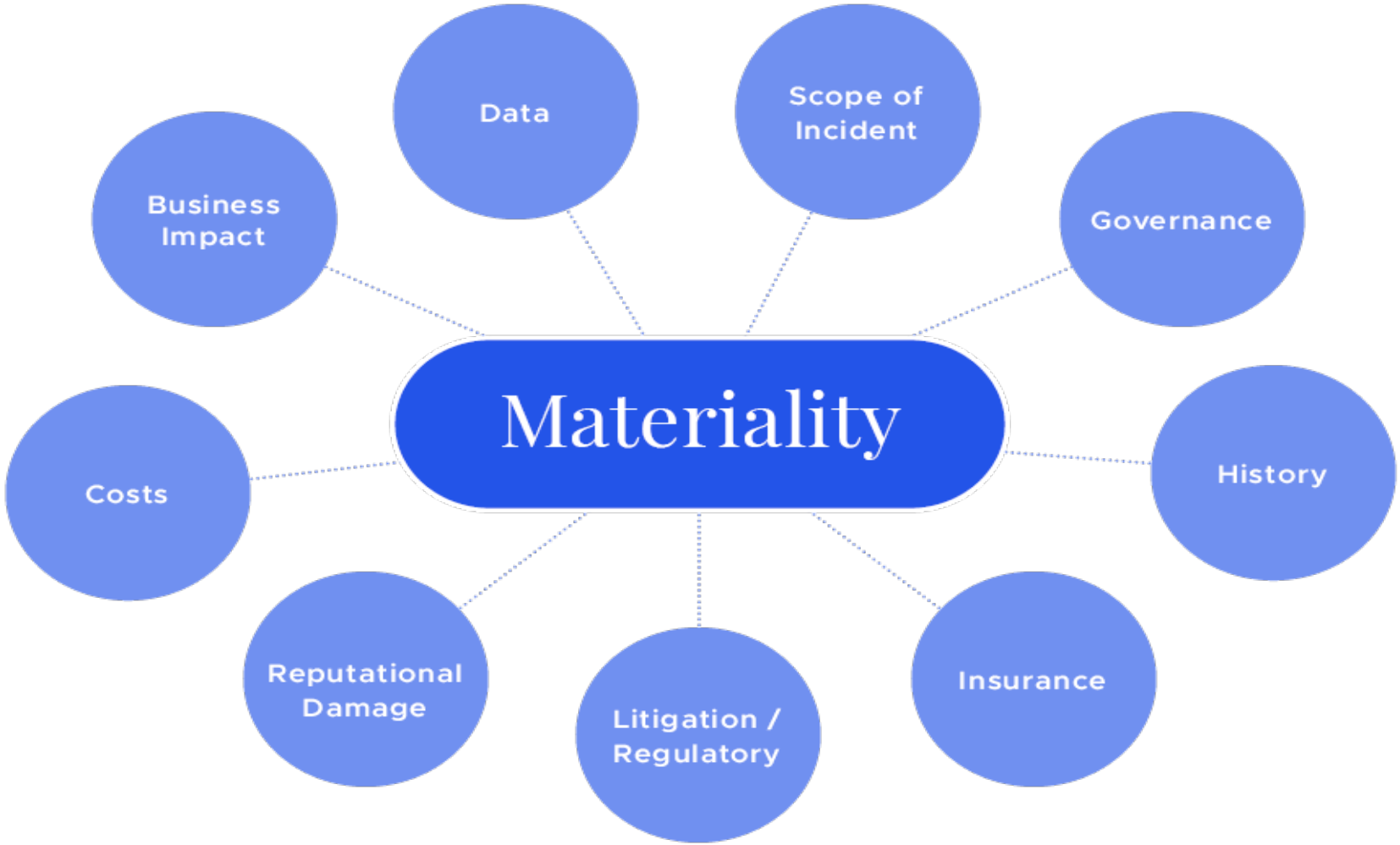
Cybersecurity Disclosures in Form 10-K

Board and Management Oversight of Cybersecurity Risks

- Describe the Board and Audit and Risk Committee's oversight of cybersecurity risks and risk management.
- Describe management's role in assessing and managing material risks from cybersecurity threats.
  - Responsibility for risk assessment and managing risks (and relevant expertise).
  - How information flows within the company regarding cybersecurity threats and incidents.
- The SEC did NOT adopt a requirement for the Board to disclose if there was a cybersecurity expert on the Board.

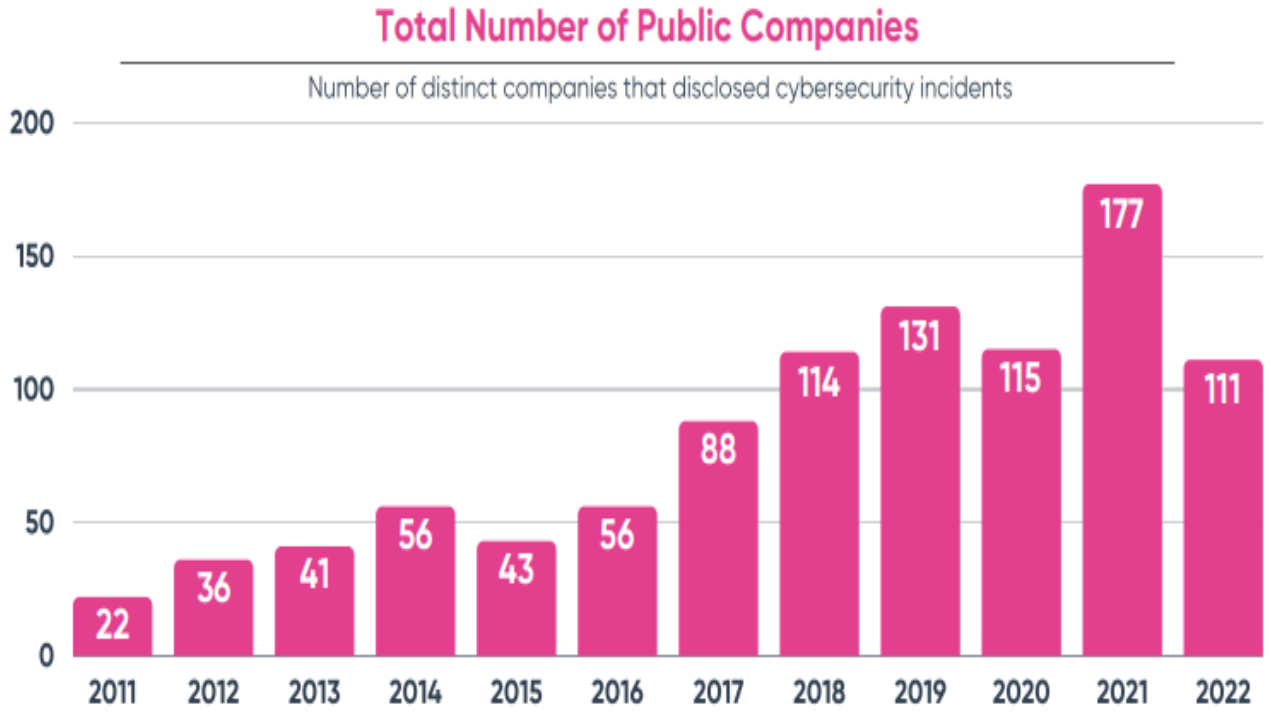
Practical Considerations

Assessing Materiality



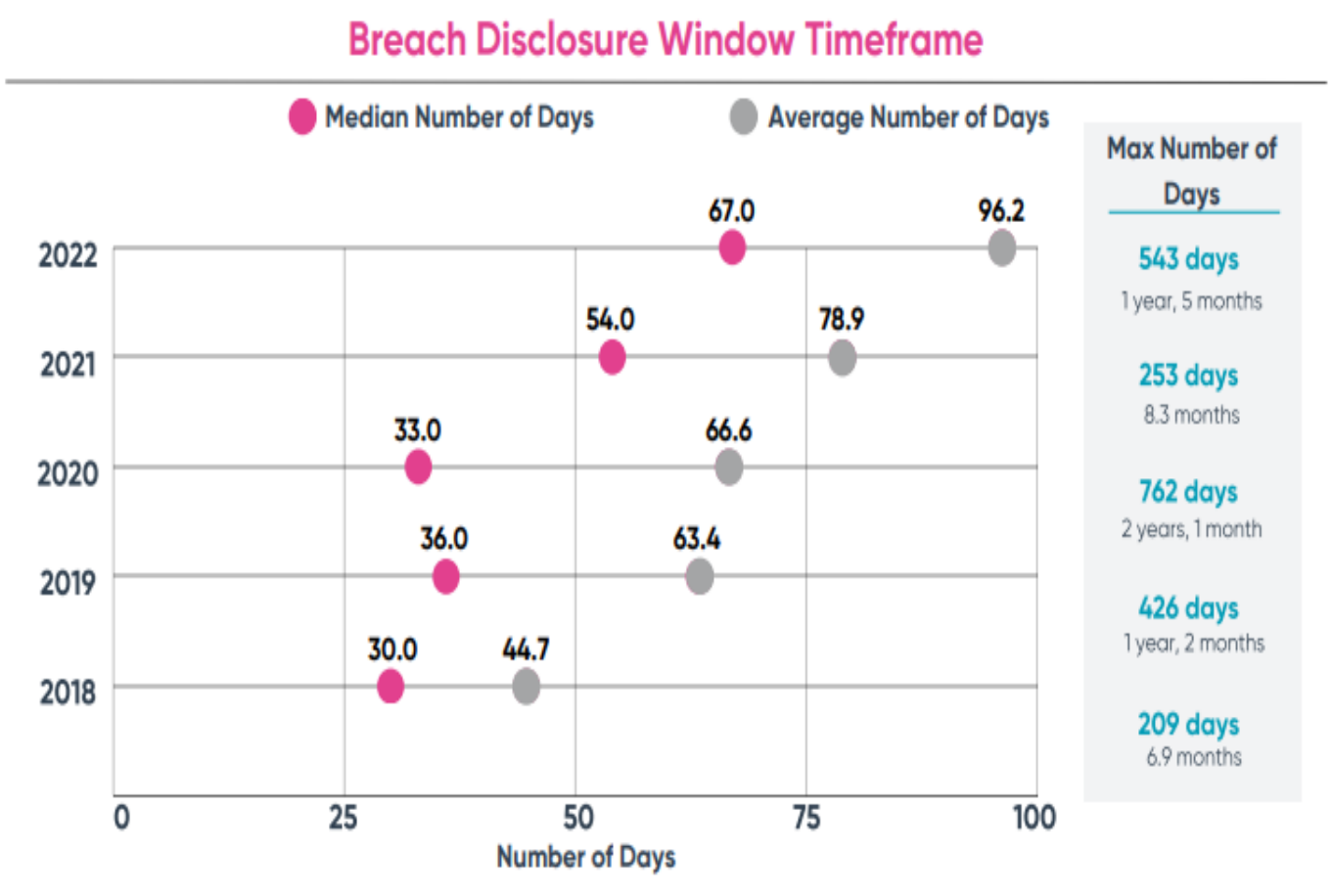
Pre-Rules Incident Reporting

- 111 companies (out of 7,000+ registrants) disclosed incidents in 2022
- 34% of these were disclosed in SEC filings. 66% were not.
- Source: Audit Analytics, "Trends in Cybersecurity Breach Disclosures" (Oct. 2023)



“Without Unreasonable Delay” + 4 Days

- In 2022, on average, 96.2 days to disclose a breach after discovery (median 67 days).
- Source: Audit Analytics, “Trends in Cybersecurity Breach Disclosures” (Oct. 2023)



Practical Considerations

- Review incident response plans and procedures to include reference to the materiality determination.
- Document a materiality process determination and materiality considerations.
- Begin discussions to update cyber risk disclosures in next 10K.
- Check D&O insurance coverage
- Note: the SEC is active in gathering information from supply chain/vendor incidents to verify whether companies are making 8Ks.

Thank you!

Kate Hanniford

Partner,

Alston & Bird

Katharine Cralle

Partner,

Brunswick Group

Julie Mediamolle

Partner,

Alston & Bird