SEC Cybersecurity “Final Rule”
Summary:

The "Cybersecurity Risk Management Strategy, Governance, and Incident Disclosure" outlines the final rules adopted by the Securities and Exchange Commission (SEC) to enhance and standardize disclosures related to cybersecurity. These rules require public companies to provide current and periodic disclosures about material cybersecurity incidents, their risk management strategies, and governance regarding cybersecurity risks. They also include guidelines on how companies should disclose the board of directors' expertise in cybersecurity and the applicability of these rules to foreign private issuers.

The document discusses the economic analysis of these rules, including their benefits, costs, and impact on efficiency, competition, and capital formation. Additionally, it addresses paperwork reduction and regulatory flexibility for small entities. The rules aim to provide investors with timely, consistent, and useful information for investment decisions while balancing the need for cybersecurity protection.

(please see the next page)

Item	Summary description of the disclosure requirement [30]
Regulation S–K Item 106(b)— *Risk management and strategy*	Registrants must describe their processes, if any, for the assessment, identification, and management of material risks from cybersecurity threats, and describe whether any risks from cybersecurity threats have materially affected or are reasonably likely to materially affect their business strategy, results of operations, or financial condition.
Regulation S–K Item 106(c)— *Governance*	Registrants must: —Describe the board's oversight of risks from cybersecurity threats. —Describe management's role in assessing and managing material risks from cybersecurity threats.
Form 8–K Item 1.05— *Material Cybersecurity Incidents*	Registrants must disclose any cybersecurity incident they experience that is determined to be material, and describe the material aspects of its: —Nature, scope, and timing; and —Impact or reasonably likely impact. An Item 1.05 Form 8–K must be filed within four business days of determining an incident was material. A registrant may delay filing as described below, if the United States Attorney General ("Attorney General") determines immediate disclosure would pose a substantial risk to national security or public safety. Registrants must amend a prior Item 1.05 Form 8–K to disclose any information called for in Item 1.05(a) that was not determined or was unavailable at the time of the initial Form 8–K filing.
Form 20–F	FPIs must: —Describe the board's oversight of risks from cybersecurity threats. —Describe management's role in assessing and managing material risks from cybersecurity threats.
Form 6–K	FPIs must furnish on Form 6–K information on material cybersecurity incidents that they disclose or otherwise publicize in a foreign jurisdiction, to any stock exchange, or to security holders.

This Final Rule further elaborates on the specific requirements for disclosures related to cybersecurity incidents, detailing the nature, extent, and potential materiality of these incidents. It emphasizes the need for companies to regularly review and update their cybersecurity policies and strategies, reflecting the evolving nature of cyber threats. Additionally, the document highlights the role of corporate governance in managing cybersecurity risks, including the involvement of the board of directors and management. The SEC's aim with these rules is to provide a comprehensive framework that ensures

public companies are more transparent about their cybersecurity practices and incidents, ultimately enhancing investor confidence and market integrity.

Certainly, here's a comprehensive summary combining the information from both responses:

1. Cybersecurity Incident Disclosure:

- The Rule mandates immediate disclosure of cybersecurity incidents that are material.
- Disclosures should include specifics like the nature and scope of the incident, the impact on operations, and remedial actions taken.
- Statistics: As of May 2022, disclosures of efforts to mitigate cybersecurity risk were found in 99% of proxy statements or Forms 10-K, up from 93% in 2020 and 85% in 2018.
- Importance: The increasing rate of disclosures reflects the growing emphasis on cybersecurity risk management among large companies.

2. Risk Management Strategy:

- Companies must outline their strategies for identifying and managing cybersecurity risks.
- This includes integrating cybersecurity risks into the company's broader risk management.
- Example: A company might describe its process for regularly assessing cybersecurity threats and its protocols for mitigating such risks.

3. Governance:

- The Rule emphasizes the role of corporate governance, especially the board of directors, in overseeing cybersecurity risks.
- Companies are required to disclose how their boards oversee and evaluate cybersecurity risk management.
- Example: A disclosure might include whether any board members have cybersecurity expertise and how the board engages with cybersecurity issues.

4. Economic Analysis:

- The Rule discusses the potential economic impacts of the new disclosure requirements.
- It weighs the benefits of increased transparency against the costs of compliance.
- Example: The Rule might analyze the cost for companies to implement new cybersecurity reporting systems versus the benefit to investors from more transparent information.

5. Investor Protection:

- The SEC aims to protect investors by mandating detailed disclosures about cybersecurity.
- These disclosures are intended to provide investors with timely information for informed decision-making.
- Example: Investors can use information about a company's cyber incident response to assess the company's overall risk management efficacy.

6. **Regulatory Flexibility:**

- The Rule considers the impact on smaller entities, offering some compliance flexibility.
- It addresses concerns like the paperwork burden and potential cost of compliance for smaller companies.
- Statistics: The Rule details the estimated changes in annual responses, burden hours, and costs for various forms like Form 8-K and Form 10-K. For instance, Form 8-K shows an increase of 200 annual responses and 1,350 burden hours, with a cost increase of $270,000.
- Importance: This flexibility and detailed breakdown help smaller companies manage the impact of these new regulations.

In conclusion, the SEC's Rule represents a significant step forward in enhancing the transparency and accountability of public companies in the realm of cybersecurity. By mandating detailed disclosures of material cybersecurity incidents and the strategies for managing such risks, the Rule acknowledges the critical importance of cybersecurity in today's digital age. The inclusion of comprehensive statistics, such as the finding that 99% of proxy statements or Forms 10-K included disclosures of efforts to mitigate cybersecurity risk as of May 2022, up from 93% in 2020 and 85% in 2018, underscores the increasing recognition of cybersecurity's role in corporate governance and risk management.

Moreover, the Rule's emphasis on the economic analysis of these new requirements, balancing the benefits of increased investor transparency with the compliance costs for companies, reflects a nuanced understanding of the complexities involved in cybersecurity reporting. The SEC's approach, particularly its consideration of the impact on smaller entities and the provision of regulatory flexibility, demonstrates a thoughtful and measured response to the evolving cybersecurity landscape. The detailed breakdown of the changes in annual responses, burden hours, and costs for various forms, such as Form 8-K and Form 10-K, highlights the SEC's commitment to ensuring that these new regulations are manageable and effective across the spectrum of public companies.