BLANKROME

Privacy, Security & Data Protection

AUGUST 7, 2023 • NO. 2

Brave New World for Cybersecurity Risk Management and Incident Disclosure

The Securities and Exchange Commission ("SEC") recently adopted new rules to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident disclosure by public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934. In light of these new rules, public and private companies alike need to be vigilant about their internal controls and accountability regarding cybersecurity incidents, which seem to happen daily. A company's policies and procedures that would enable it to identify cybersecurity risks and incidents are table stakes for all businesses today.

Specifically, on July 26, 2023, the SEC:

- revised Current Report on Form 8-K by adding new Item 1.05, *Material Cybersecurity Incidents,* to be filed within four business days after the company determines that it has experienced a material cybersecurity incident, but the untimely filing of an Item 1.05 Form 8-K will not result in the loss of Form S-3 eligibility;

- revised Annual Report on Form 10-K by adding new Item 1C, *Cybersecurity,* to Part I of Form 10-K, in which a public company would need to provide information required by the new Item 106 of Regulation S-K, which focuses on disclosures about a company's processes to assess, identify, and manage material cybersecurity risks, management's role in assessing and managing material cybersecurity risks, and the board of directors' oversight of cybersecurity risks; and

- required Form 8-K and Form 10-K cybersecurity disclosures to be provided in Inline eXtensible Business Reporting Language ("Inline XBRL").

The new rules also require comparable disclosures by foreign private issuers in (i) Form 6-K with respect to material cybersecurity incidents that they disclose or otherwise publicize in a foreign jurisdiction, to any stock exchange, or to security holders and (ii) Form 20-F regarding cybersecurity risk management, strategy, and governance.

In order for public companies to make disclosures mandated by the new rules, they will need to flow down the SEC cybersecurity requirements to their suppliers and partners, which will enable cybersecurity risk management across the larger marketplace. Contracts will require representations about the suppliers' cyber maturity and potentially termination of contracts in the event of a cyber incident caused by noncompliance. Communication, transparency, and collaboration about cybersecurity risks up and down the supply chain will be essential to mitigate business continuity risk. The new SEC rules underscore the fact that cybersecurity is a business problem, not just an IT issue, which mandates proactive attention.

NEW ITEM 1.05 OF FORM 8-K CONTAINS THE FOLLOWING REQUIREMENTS:

- If the company experiences a cybersecurity incident[1] that is determined by the company to be material[2], it must describe the material aspects of the nature, scope, and timing of the incident and the material impact or reasonably likely material impact on the company, including its financial condition and results of operations.[3]

- However, the company does not need to disclose specific or technical information about its planned response to the incident or its cybersecurity systems, related networks and devices, or potential system vulnerabilities in such detail as would impede the company's response or remediation of the incident.

- Notwithstanding the requirement to file Form 8-K within four business days after the company *determines* that it has experienced a material cybersecurity incident, if the United States Attorney General determines that the disclosure required above poses a substantial risk to national security or public safety, and notifies the SEC of such determination in writing, the company may delay providing the disclosure required by Item 1.05 for a time period specified by the Attorney General, up to 30 days following the date when the disclosure required by Item 1.05was otherwise required to be provided.

- Disclosure may be delayed for an additional period of up to 30 days if the Attorney General determines that disclosure continues to pose a substantial risk to national security or public safety and notifies the SEC of such determination in writing.

- In extraordinary circumstances, disclosure may be delayed for a final additional period of up to 60 days if the Attorney General determines that disclosure continues to pose a substantial risk to national security and notifies the SEC of such determination in writing.

- Beyond such final 60-day delay, if the Attorney General indicates that further delay is necessary, the SEC will consider additional requests for delay and may grant such relief through SEC exemptive order.

Notwithstanding the requirement to file Form 8-K within four business days after the company *determines* that it has experienced a material cybersecurity incident, if a company that is subject to 47 CFR 64.2011[4] is required to delay disclosing a data breach pursuant to such rule, it may delay providing the disclosure required by Item 1.05 for such period that is applicable under 47 CFR 64.2011(b)(1) and in no event for more than seven business days after notification required under such provision has been made, so long as the company notifies the SEC through correspondence submitted to the EDGAR system no later than the date when the disclosure required by Item 1.05 was otherwise required to be provided.

NEW ITEM 106 OF REGULATION S-K TO BE REPORTED IN FORM 10-K CONTAINS THE FOLLOWING REQUIREMENTS:

- *Disclose the company's cybersecurity risk management and strategy by describing:*

  (1) the company's processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats[5] in sufficient detail for a reasonable investor to understand those processes by addressing, as applicable, the following non-exclusive list of disclosure items:

  (i) whether and how any such processes have been integrated into the company's overall risk management system or processes;

  (ii) whether the company engages assessors, consultants, auditors, or other third parties in connection with any such processes; and

  (iii) whether the company has processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider.

  (2) 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.

- *Disclose the company's governance related to cybersecurity matters by describing:*

  (1) the board of directors' oversight of risks from cybersecurity threats, and, if applicable, identifying any board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and describing the processes by which the board or such committee is informed about such risks.

(2) management's role in assessing and managing the company's material risks from cybersecurity threats and addressing, as applicable, the following non-exclusive list of disclosure items:

(i) whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise (where such relevant expertise may include, for example: prior work experience in cybersecurity; any relevant degrees or certifications; any knowledge, skills, or other background in cybersecurity);

(ii) the processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents; and

(iii) whether such persons or committees report information about such risks to the board of directors or a committee or subcommittee of the board of directors.

COMPLIANCE DATES ARE AS FOLLOWS:

- The new rules are effective on September 5, 2023.
- All companies must provide disclosures required in annual reports on Form 10-K or Form 20-F beginning with annual reports for fiscal years ending on or after December 15, 2023.
- All companies, other than smaller reporting companies, must begin complying with the incident disclosure requirements in Item 1.05 of Form 8-K and in Form 6-K on December 18, 2023. Smaller reporting companies must begin complying with Item 1.05 of Form 8-K on June 15, 2024.
- All companies must tag required disclosures in Inline XBRL in (i) annual reports on Form 10-K or Form 20-F beginning with annual reports for fiscal years ending on or after December 15, 2024, and (ii) in Form 8-K or 6-K beginning on December 18, 2024.

For more information or assistance, contact Yelena Barychev, Sharon Klein, or another member of Blank Rome's Corporate or Privacy, Security & Data Protection groups.

Yelena M. Barychev
215.569.5737 | yelena.barychev@blankrome.com

Sharon R. Klein
949.812.6010 | sharon.klein@blankrome.com

---

1. The term "cybersecurity incident" means 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. (See Item 106(a) of Regulation S-K)

   The term "information systems" means electronic information resources owned or used by the company, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the company's information to maintain or support the company's operations. (See Item 106(a) of Regulation S-K)

2. Instruction 1 to Item 1.05 states that "a company's materiality determination regarding a cybersecurity incident must be made without unreasonable delay after discovery of the incident."
3. Instruction 2 to Item 1.05 states that, to the extent that the information called for in Item 1.05(a) is not determined or is unavailable at the time of the required filing, the company must include a statement to this effect in the initial Form 8-K filing and then must file an amendment to Form 8-K containing such information within four business days after (i) the company, without unreasonable delay, determines such information, or (ii) such information becomes available.
4. 47 CFR 64.2011 provides federal agencies broad jurisdiction in data breach notification. The Federal Trade Commission's expertise in consumer protection is often called upon by other agencies such as the SEC to assist in determination of adequate notification.
5. The term "cybersecurity threat" means 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. (See Item 106(a) of Regulation S-K)