DIGITAL DIRECTORS NETWORK

CHEATLIST
SEC CYBERSECURITY
DISCLOSURE REQUIREMENTS

REQUIRED FORM 8-K CURRENT REPORT DISCLOSURES: MATERIAL CYBERSECURITY INCIDENTS [1]
Upon determining that a cybersecurity incident (unauthorized or accidental occurrence) is material to a reasonable investor, SEC registrants are required to disclose the following information within 4-business days as long as it is not an issue of national security or public safety as determined by the U.S. Department of Justice.[2]
☐ Describe the material aspect of the nature, scope, and timing of the incident.[3]
☐ Describe the material impact or reasonably likely material impact on the registrant, including (non-exclusively) financial condition and results of operations along with qualitative factors such as harm to reputation, customer of vendor relationships, competitiveness, litigation, U.S. and non-U.S. regulatory investigations, etc.
☐ Disclose updated [material] incident information within four business days, after the registrant, without unreasonable delay, determines such information or within four business days after such information becomes available in a Form 8-K amendment.

[1] Cybersecurity incident means an unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein. **Accidental occurrences are also an unauthorized occurrence.** Information system means electronic information systems owned or used by registrant, 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 registrant's information to maintain or support the registrant's operations. Materiality determination is be made without unreasonable delay.

[2] If at any time incident is deemed to be in the interest of national security or public safety, the FBI is to be contacted to begin the process for disclosure delay consideration. Otherwise, disclosure is due within 4-business days of determining it is material to a reasonable investor. https://www.fbi.gov/investigate/cyber/fbi-guidance-to-victims-of-cyber-incidents-on-sec-reporting-requirements

[3] Disclosure does not need to include "specific or technical information about its [registrants] planned response to the incident or its cybersecurity systems, related networks and devices, or potential system vulnerabilities in such details as would impede the registrant's response or remediation of the incident."

REQUIRED FORM 10-K ANNUAL REPORT DISCLOSURES: RISK MANAGEMENT, STRATEGY AND GOVERNANCE OF CYBERSECURITY RISKS
RISK MANAGEMENT AND STRATEGY
Registrants are now required to provide more consistent and informative disclosure regarding their cybersecurity risk management and strategy in their annual reports, Form 10-K, by:
☐ Describing the registrant'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.[4] The enumerated elements, non-exclusively,[5] that a registrant should specifically address within this disclosure include:
☐ Whether the above processes have been integrated into the registrant's overall risk management processes;

☐ Whether the registrant engages assessors, consultants, auditors, or other third parties in connection with any such processes;
☐ Whether the registrant has processes to oversee and identify **material** risks from cybersecurity threats associated with its use of any third-party service provider and other information necessary for a reasonable investor to understand their cybersecurity processes.
☐ Describing 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 registrant, including its business strategy, results of operations, or financial condition and if so, how.
MANAGEMENT'S ROLE AND CORPORATE GOVERNANCE
☐ Describing the board's oversight of risks from cybersecurity threats.
☐ Including, if applicable, identifying and describing if any board committee, or subcommittee is responsible for such oversight
☐ Describing the processes by which the board or such committee is informed about such risks
☐ Describing management's role in assessing and managing the registrant's **material** risks from cybersecurity threats including describing (non-exclusively):
☐ Whether and which management position or committees are responsible for assessing and managing such risks, and
☐ The relevant expertise of such person or members in such detail as necessary to fully describe the nature of the expertise.[6]
☐ 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 such risks to the board of directors or a committee or subcommittee of the board.

[4] Processes are not policies and procedures. This context is intended to allow registrants to avoid operational details that may advantage threat actors and exacerbate risk. The SEC expects this disclosure to be sufficient enough to allow investors to ascertain a registrant's cybersecurity practices, such as whether they have a risk assessment program in place, with sufficient details for investors to understand the registrant's cybersecurity risk profile, i.e. risk appetite and tolerances.

[5] Registrants should additionally disclose whatever information is necessary based on their facts and circumstances for a reasonable investor to understand their cybersecurity processes.

[6] Prior work experience in cybersecurity; any relevant degrees or certifications; any knowledge, skills, or other background in cybersecurity.