CyberSecurity Risk Management

An Overview

October 2023

A Presentation for Florida State University College of Law

New SEC Disclosure Rules… What's Different?

Final rules implement same basic structure as initially proposed (2022) – namely:

- Disclosures of cyber risk management, strategy, and governance in annual reports; and
- Reporting required for ***material*** cybersecurity incidents on Form 8-K or Form 6-K.

SEC noted that registrant disclosures of material cybersecurity incidents and cybersecurity risk management and governance have improved since the 2011 and 2018 guidance, however the Commission "remain[s] persuaded that…under-disclosure regarding cybersecurity persists despite…prior guidance" and "investors need more timely and consistent cybersecurity disclosure to make informed investment decisions."

© 2023 Grant Thornton LLP | All rights reserved | U.S. member firm of Grant Thornton International Ltd

Annual Disclosures…

- The Final Rule amends Form 10-K (via new Item 106 of Regulation S-K) to require registrants to disclose information about cyber risk management, strategy, and governance.
- **Risk Management & Strategy**:
  - Company processes for the assessment, identification, and management of material risks from cybersecurity threats;
  - Commentary on whether any of these risks (including prior cyber incidents) have materially affected (or are reasonably likely to materially affect) business strategy, results of operations, or financial condition – and, if so, how;
  - Description of whether and how such processes have been integrated into the registrant's overall risk management system or processes;
  - Registrant's use of assessors, consultants, auditors, or other third-parties in connection with such processes; and
  - Commentary on whether the registrant has processes to oversee and identify material risks from cybersecurity threats associated with its use of any third-party service provider.

© 2023 Grant Thornton LLP | All rights reserved | U.S. member firm of Grant Thornton International Ltd

Annual Disclosures (Board Governance)…

- **Board Oversight**
  - Final rules require registrants to describe the of risks from cybersecurity threats – including, *if applicable*:
    - identification of any board committee or subcommittee responsible for the oversight of such risks; and
    - a description of the processes by which the board or such committee is informed about such risks.
  - Notably, SEC did *NOT* adopt the proposed requirement to disclose board cybersecurity expertise.
  - Likewise, the new governance disclosure provisions do *NOT* require disclosure of the frequency of management and board discussions regarding cybersecurity risks, which had been contemplated by the proposed rules.

© 2023 Grant Thornton LLP | All rights reserved | U.S. member firm of Grant Thornton International Ltd

Annual Disclosures (Management)…

- **Management Oversight**
  - Requirement to describe management's role in assessing and managing material risks from cybersecurity threats, including relevant expertise and communication with the board of directors.
  - Item 106(b) of Regulation S-K includes (non-exclusive) list of disclosure items:
    - management positions responsible for assessing/managing cybersecurity risks;
    - relevant expertise of such persons;
    - processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation, and remediation of cybersecurity incidents; and
    - whether such persons or committees report information about such risks to the board or a committee or subcommittee of the board.

© 2023 Grant Thornton LLP | All rights reserved | U.S. member firm of Grant Thornton International Ltd

Incident Disclosures…

Final Rule adds Item 1.05 to Form 8-K, requiring disclosure of the nature, scope, and timing of a material cybersecurity incident – as well as the material impact (or reasonably likely material impact) of the incident.

Key Insights (for disclosure and materiality committees):

1. A materiality determination must occur *without unreasonable delay*.
2. Reporting required within 4 business days of materiality determination (via 8-K);
3. Limited delayed-disclosure exceptions (national security + public safety risks);
4. 8-K disclosure must focus on the impacts of the incident;
5. Updated incident disclosure is required (as issues become known/clarified); and
6. Importantly, the final rules do *NOT* embrace the proposed requirement to disclose a series of previously undisclosed, individually immaterial incidents (unless such incidents comprise a “series of related unauthorized occurrences”)*.

* This presupposes the tracking of minor cyber incidents for potential aggregation.

© 2023 Grant Thornton LLP | All rights reserved | U.S. member firm of Grant Thornton International Ltd

Sample 8-K Cyber Disclosures

Company Name	Incident Type	Disclosure Date	Filing
Blackbaud Inc.*	Ransomware	07/16/2020	8-K
PGT Innovations	Ransomware	11/07/2022	8-K
Belden Inc.	PII Compromise	11/27/2020	8-K
QuickLogic Corp.	General	03/14/2023	8-K
Heico Corp.	General / Theft	04/12/2023	8-K
Brunswick Corp.	General	06/14/2023	8-K / Press Release

* In March 2023, the SEC fined Blackbaud $3 million fine for its allegedly misleading disclosures that the SEC contended underplayed the extent and impact of the 2020 ransomware attack

Grant Thornton

© 2023 Grant Thornton LLP | All rights reserved | U.S. member firm of Grant Thornton International Ltd

Grant Thornton

Board Engagement

October 2023

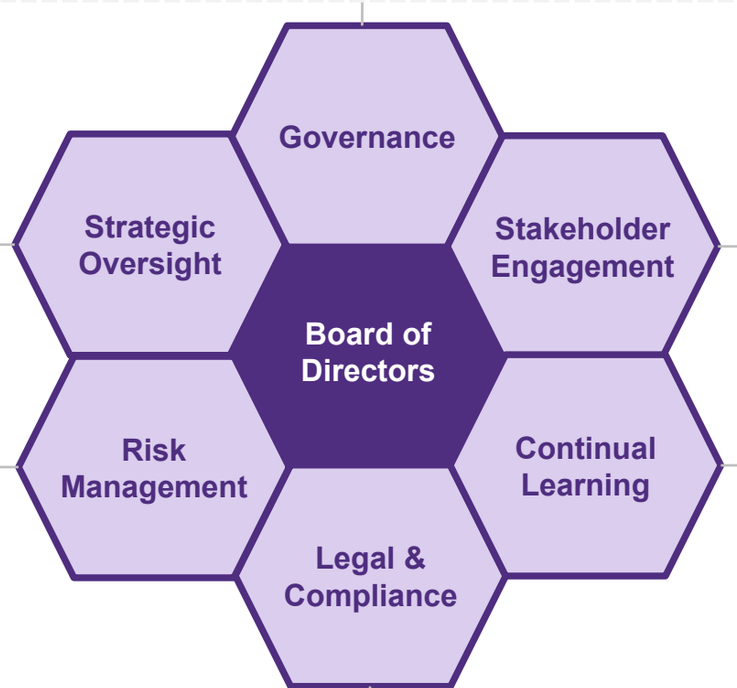
Board of Directors Role in CyberSecurity Oversight…

The Board plays a critical role in the management of cyber risk through via **risk management, governance, and strategy**

Ensure proper controls, monitoring, reporting & structure to oversee the company's risk management

Is Cyber considered a category of Enterprise Risk (versus an "IT Domain")?

Ensure a robust risk management framework to help identify, assess, and mitigate cyber risks



Determine impact on stakeholders (internal and external) and ensure open communication with same

Board education should be ongoing, specifically around emerging cyber threats and their implications

Understand legal and regulatory compliance mandates (disclosure, notice periods, reporting channels)

Grant Thornton

© 2023 Grant Thornton LLP | All rights reserved | U.S. member firm of Grant Thornton International Ltd

What Questions should the Board be asking?

Current State

- What is the company's process for assessing and managing material risks from cyber threats?
- How does the company coordinate cyber incident response with the broader business?
- Which third-parties are used to help manage cyber risk in our environment?
- Which third-party vendors/partners (were they to be attacked) represent potentially material exposures?

Strategic Focus

- How will management apprise the Board on emerging and persistent cyber risks?
- What has management done to ensure that we have the right expertise to manage cyber risk?
- How does management ensure that the company has resilience against cyber-attacks?
- What resources are needed most by management to manage cyber risk?
- How does the business measure and monitor third-party cyber risk?
- Is our current insurance coverage sufficient? How does management know as much?
- Does the organization have the required governance policies and controls in place? How will we enforce new policies and procedures?

© 2023 Grant Thornton LLP | All rights reserved | U.S. member firm of Grant Thornton International Ltd

Board Governance Landscape (Cyber)

The Board should establish oversight across the following categories of cyber risk management.

Oversight Mechanisms (General)	Guidance regarding the fundamental avenues through which the Board understands issues related to cybersecurity.
Review Policies, Procedures & Resources	Guidance for the Board in overseeing management's development and maintenance of the foundation of a mature cybersecurity program.
Verify Risk Identification & Assessment	Guidance for what the Board should know about management's plan to measure and mitigate cybersecurity risk.
Oversight of Protection, Detection & Mitigation Plans	Guidance for the Board's oversight of management's program for guarding against and remediating potential cyber threats and vulnerabilities.
Oversight of Incident Response & Disclosure Strategy	Guidance regarding the Board's role in preparation for and following the response to a cybersecurity incident.
Documentation of Board Oversight	Guidance related to requirements for documenting the Board's oversight activities.

© 2023 Grant Thornton LLP | All rights reserved | U.S. member firm of Grant Thornton International Ltd

Board Oversight Categories (Cyber)

Regardless of the governance model selected by a company, the Board needs to achieve the following criteria to satisfy its governance and fiduciary responsibilities:

Oversight Mechanisms (General) – The Board should:

- Ensure that cybersecurity considerations are a recurring agenda item for full Board meetings;
- Consider the appointment of Directors with cybersecurity experience;
- Engage in ongoing Director education on these matters;
- Periodically review management-level systems and reporting structures to ensure effectiveness;
- Periodically review enterprise-wide cybersecurity programs to ensure that they contemplate all business units and legacy assets – as well as newly acquired or developed businesses/assets.
- Request that management demonstrate how cybersecurity considerations extend to a company's supply chain, vendor, and business partner relationships – including business initiatives involving new markets, new digital platforms, and material changes to business models and operational structures;
- Consider when and how expert third-party firms will be used as part of the company's cyber risk efforts; and
- Consider what kind of periodic reports and analysis (including from third-party firms) are provided to the Board, relevant committee(s), and/or senior management.

© 2023 Grant Thornton LLP | All rights reserved | U.S. member firm of Grant Thornton International Ltd

Board Oversight Categories – Cyber (cont.)

Review Policies, Procedures and Resources – The Board should:

- Ensure that the company has written policies and procedures governing each of the elements outlined in NIST CSF;
- Ensure that both the cybersecurity and internal audit functions are adequately resourced (especially related to risk-related responsibilities, technical expertise, and sufficient time to devote to cybersecurity risk and review);
- Review the common elements of cyber-related enforcement actions brought by state and federal actors; and
- Review the company's written information security programs and digest senior management Board presentations (on at least an annual basis).

Verify Risk Identification and Assessment – The Board should:

- Work to understand the mission-critical systems used by the company uses, the data it collects, as well as the risks related to how the company uses technology and collects/stores data;
- Ensure that a cyber risk assessment and mitigation system is in place at the company (including treatment of risks that may materially affect business strategy, results of operations, and/or financial condition);
- Ensure that those managing the company's cybersecurity consider potential vulnerabilities (by leveraging the latest threat-intelligence and best practices); and
- Memorialize the oversight it exercises of management's risk assessments and the Committee(s) overseeing same.

© 2023 Grant Thornton LLP | All rights reserved | U.S. member firm of Grant Thornton International Ltd

Board Oversight Categories – Cyber (cont.)

Oversight of Protection, Detection and Mitigation Plans – The Board should:

- Consume consistent quarter-to-quarter reporting and briefings from CISO (or equivalent) to delve into issues related to management's plans to implement appropriate protections against cyber intrusions and related risks – including programmatic efforts to detect and mitigate vulnerabilities and enable business continuity;
- Understand whether Management remediates material cyber risks in a timely fashion;
- Understand which personnel are responsible for continuous monitoring and improvement efforts; and
- Determine which employees from the internal audit function are involved in the management of cyber risk.

Oversight of Incident Response & Disclosure Strategy – The Board should:

- Request periodic briefings on management's procedures to facilitate swift and effective response to a cybersecurity incident (including unlikely events with material consequences);
- Confirm that management's response plan includes notification provisions and response protocols for various crisis scenarios – including escalation steps to incorporate key business stakeholders into materiality considerations;
- Understand management's program for determining materiality for cyber incidents and the protocols to file required disclosures in the mandated timeframe for material events;

© 2023 Grant Thornton LLP | All rights reserved | U.S. member firm of Grant Thornton International Ltd

Board Oversight Categories – Cyber (cont.)

Oversight of Response Strategy and Disclosure (cont'd) – The Board should:

- Require briefings on management's response to material incidents, the status of investigations, and whether the response plan was effective, and if management recommends material changes to the plan or systems following an event;
- Understand the process by which management determines whether an event (or a series of related events) are material, the criteria for determining materiality, the management team responsible for making that determination, and the Board's role in that materiality process; and
- Understand by which mechanisms management would notify law enforcement and/or state or federal agencies for matters related to national security or other serious matters.

Documentation of Board Oversight – The Board should:

- Document the oversight activities of Board (and/or committees) within its minutes and supporting materials, given the increasing likelihood that such documentation may be made accessible via stockholder-inspection, regulatory, or litigation-related demands.

© 2023 Grant Thornton LLP | All rights reserved | U.S. member firm of Grant Thornton International Ltd

Todd McClelland
McDermott Will & Emery LLP
Partner & Global Head of
Privacy & Cybersecurity Practice

tmcclelland@mwe.com

Johnny Lee
Grant Thornton LLP
Principal & National Practice Leader,
Forensic Technology

j.lee@us.gt.com

www.grantthornton.com

twitter.com/GrantThorntonUS

Thank you!