CAC Specialty™

APRIL 2022 CLIENT ALERT

CYBER-RISK TRANSLATES INTO HEIGHTENED D&O RISK

Recently, the SEC has proposed rules and amendments to previous guidance on cybersecurity reporting requirements for public companies. The stated goals of the proposed regulations are: (i) the consistent and timely disclosure of cyber incidents; (ii) requirement of the board and management team of public companies to understand materiality in financial terms of a breach before a breach occurs; (iii) deployment of continuous breach/cyber event monitoring solutions and (iv) measures that would require companies to identify service providers that could pose cybersecurity risks and hold organizations accountable for a service provider's lack of cybersecurity measures. All of the aforementioned considerations continue to raise the bar as respects potential obligations and liability of directors and officers.

See below excerpt from the Harvard Law School Forum on Corporate Governance post on April 11th summarizing the proposed rules (click HERE for full post):

> *What these prior Commission statements and litigation releases failed to deliver on, the new proposed rules significantly raise the bar on. These proposed rules appreciably increase corporate accountability on cyber risk from the boardroom on down. By becoming more specific and prescriptive the SEC is addressing observed shortcomings and inconsistencies in cyber incident reporting practices that range from whether an incident is even disclosed, what gets disclosed as well as when and how companies govern and manage cyber risk. No longer just unevenly interpreted self-regulatory guidance, these are proposed regulatory changes that apply to all issuers.*
>
> *This new provision will not only require companies to understand materiality in the context of a breach, but it will have the effect of challenging boards and management teams to understand materiality in financial terms before breaches occur. Calculating projected, or expected cyber losses is something rarely done at present. But estimating this potential liability shares common ground with any estimate of probable and estimable losses such as loan loss reserves for banks, warranty liabilities for manufacturers or doubtful accounts receivable for any company.*
>
> *Whereas corporate leadership may have felt that cyber insurance effectively transferred the majority of their risk exposure to a third-party, the reality of the expanding impacts of cyber risk means that issuers are primarily self-insured for the significant majority of the cyber risks and costs that they face. This proposed change will now force corporate boards and management to have a new understanding of the far-reaching economic impacts inherent within their cyber risk environment, the specifics of their cyber control practices and policies from the boardroom down, and the specific impacts of a breach.*

The National Association of Corporate Directors (NACD), SecurityScorecard and Cyber Threat Alliance jointly endorse the proposed rules (HERE), concluding that they "would strengthen the ability of public companies, Funds and Advisors to combat cybersecurity threats and implement risk mitigation processes". From the full report:

> ***Role of the Board:*** Companies should be aware that legislators and regulators are becoming increasingly focused on the role of boards in preventing, mitigating, and, where necessary, disclosing cybersecurity incidents. Directors should take an active role in ensuring processes are in place that are designed to appropriately escalate cybersecurity issues within the company and should be prepared to critically assess their organization's cybersecurity readiness posture both internally and with respect to third-and fourth-party risk. Moreover, directors must understand the circumstances in which a public disclosure of a cybersecurity event is warranted and ensure that such disclosures accurately reflect the factual underpinnings of the incident. Boards should additionally take a proactive role in organizational readiness, including through discussions with relevant company stakeholders on potential policy or process gaps.

We anticipate that D&O underwriters will also be keenly interested in these efforts as part of their overall evaluation of a company's exposure to shareholder litigation and regulatory enforcement investigations and actions.

CAC Specialty clients have access to proprietary analytics and scenario modeling that estimate the financial exposure of a potential breach as well as unique insights into attacker infrastructure activity and preventative threat analysis via our strategic partner Cybeta Overwatch®.

CAC Specialty™

Expanding what's possible for solving risk challenges – from the simple to the previously unsolvable.

About Us **Our Solutions** **Our People** **News & Insight** **CAC Connect**