Securities Regulation Daily Wrap Up, PUBLIC COMPANY REPORTING AND DISCLOSURE—Cybersecurity firms ask SEC to adopt board-level expertise rule, (Jul 10, 2025)

By Mark S. Nelson, J.D.

The rulemaking petition sought to counter what it deemed fallacies about the originally proposed (and dropped) requirement that public companies disclose board cybersecurity expertise.

Scooter
Parts and Accessories

Digital Directors Network (DDN), a company focused on AI, digital, cybersecurity, and systemic risk governance, submitted a petition for rulemaking on behalf of a number of cyber risk firms and related interest groups, asking the Commission to include in future rulemaking a requirement that public companies disclose whether they have a cybersecurity expert on their boards of directors. As a result, the firm wants the agency to reinstate a provision that was dropped from a final regulation on public company cybersecurity disclosures. The group of firms behind the petition also includes Tenable Holdings, Inc., Allegis Cyber Capital, X-Analytics, Cyber Future Foundation, National Technology Security Coalition, HiddenLayer, Pan Asian American Business Council, AI Guardian, and the Information Systems Security Association.

Restore Item 407(j). DDN described the Commission's final public company cybersecurity regulation, which omitted the board expertise disclosure requirement, "as [providing] long overdue, common-sense, useful, and material information for investors."

But DDN said of the absence of the director disclosure provision from the Commission's final regulation: "There is no mitigating control for the lack of director cybersecurity expertise in the boardroom. The absence of this material cybersecurity leadership control creates a critical weakness, which evidence shows causes the boardroom to play a largely symbolic and ineffective role within the cybersecurity system, making cybersecurity less effective than it otherwise should be."

As proposed, the Commission would have required public companies to disclosure the name of any board member who had cybersecurity expertise. Expertise would be judged based on whether such person had work experience in cybersecurity, had obtained a certification or degree in cybersecurity, and whether the person had other relevant knowledge or skills, including in the areas of security policy and governance, risk management, security assessment, control evaluation, security architecture and engineering, security operations, incident handling, or business continuity planning.

Ultimately, the Commission decided not to include Item 407(j) of Regulation S-K in its final regulation. The Commission noted that board level expertise in cybersecurity could be a material disclosure, although possibly not for all investors. Instead, the Commission explained that it believed directors acting as generalists, coupled with cybersecurity disclosures required by other Commission rules would suffice.

Said the Commission: "We are persuaded that effective cybersecurity processes are designed and administered largely at the management level, and that directors with broad-based skills in risk management and strategy often effectively oversee management's efforts without specific subject matter expertise, as they do with other sophisticated technical matters."

DDN cited a number of features that it said commend the proposed rule to the Commission now. For one, the proposed rule did not mandate that companies elect new board members, but DDN said it expected many companies

© 2026 CCH Incorporated and its affiliates and licensors. All rights reserved.

would opt to bring in at least one new director with the desired cybersecurity expertise.

According to DDN, which used much of its rulemaking petition to refute what it said are false perceptions of the Commission's original proposal, the additional of cybersecurity expertise to public company boards could improve the quality of cybersecurity oversight at public companies and that in turn could reduce the cybersecurity risks many public companies face.

DDN also suggested that while many public companies do have expertise somewhere within the company regarding cybersecurity, that expertise may not necessarily be tailored to provide the kind of oversight that typically occurs at the board level. Likewise, DDN suggested that board members without specific cybersecurity expertise may be unable to adequately question and, thus, hold accountable, the company's chief information security officer (CISO).

Moreover, DDN cited a report published in 2024 by Dave DeWalt, Founder and CEO of NightDragon, that found that 12 percent of the S&P 500 have genuine cybersecurity expertise on their boards. The report suggested that only 5 percent of companies had no cybersecurity knowledge at the board level, implying that 95 percent of companies had at least some level of cybersecurity knowledge on their boards, although not necessarily direct expertise, which the report distinguished from merely being informed about a topic.

Board cyber expert not a new idea. The idea that public company boards should have some degree of cybersecurity expertise is not a new one. Senator Jack Reed (D-RI) for years has pushed lawmakers to impose a legislative requirement on public companies (a similar bill has periodically been introduced in the House). The last time the Senate version was introduced in March 2021, it garnered six cosponsors, including Sens. Susan M. Collins (R-ME) and Kevin Cramer (R-ND).

The cybersecurity board expertise disclosure, whether legislative or regulatory, would be modelled after a similar disclosure required by Item 407(d)(5) of Regulation S-K that mandates a company disclose at least one audit committee financial expert or, in the alternative, explain why the company's audit committee does not have such an expert. The audit rule was mandated by a provision contained in the Sarbanes-Oxley Act.

When the SEC adopted its cybersecurity disclosure regulation for public companies, Sen. Reed lamented the Commission's decision to omit the board expertise disclosure requirement from the final version of the regulation.

"The SEC's original proposal would have implemented this bipartisan legislation," said Sen. Reed. "But the SEC has watered down the rule by requiring general disclosure of the board's oversight of cyber risk, without requiring specific disclosure of directors' qualifications regarding cybersecurity."

Senator Reed said at the time that he remained committed to seeking a board cybersecurity expertise disclosure requirement and, regarding the Commission's chosen path, added: "While this approach is an improvement, it does not provide appropriate incentives for companies to proactively address cyber risk. It also leaves investors without critical information about cyber expertise at the highest level of public companies."

The DDN rulemaking petition to add a board cybersecurity expertise disclosure also comes at a time when the SEC has recently withdrawn existing cybersecurity proposals in three areas, signaling a possible retreat from or future re-write of existing cybersecurity disclosure rules. The three areas addressed by the formally withdrawn proposals are: (1) cybersecurity rules for investment advisers, registered investment companies, and business development companies; (2) amendments to Regulation Systems Compliance and Integrity; and (3) cybersecurity rules for a variety of market participants, including broker-dealers, clearing agencies, major security-based swap participants, and self-regulatory organizations.

Companies: Digital Directors Network on behalf of Tenable Holdings, Inc.; Allegis Cyber Capital; X-Analytics; Cyber Future Foundation; National Technology Security Coalition; HiddenLayer; Pan Asian American Business Council; AI

© 2026 CCH Incorporated and its affiliates and licensors. All rights reserved.

Guardian; Information Systems Security Association

MainStory: TopStory CorporateGovernance CyberPrivacyFeed DataSecurity DirectorsOfficers FedTracker Securities InvestorEducation PublicCompanyReportingDisclosure RiskManagement

© 2026 CCH Incorporated and its affiliates and licensors. All rights reserved.

Nov 20, 2026 from VitalLaw®