by **Evan Schuman**
Contributor

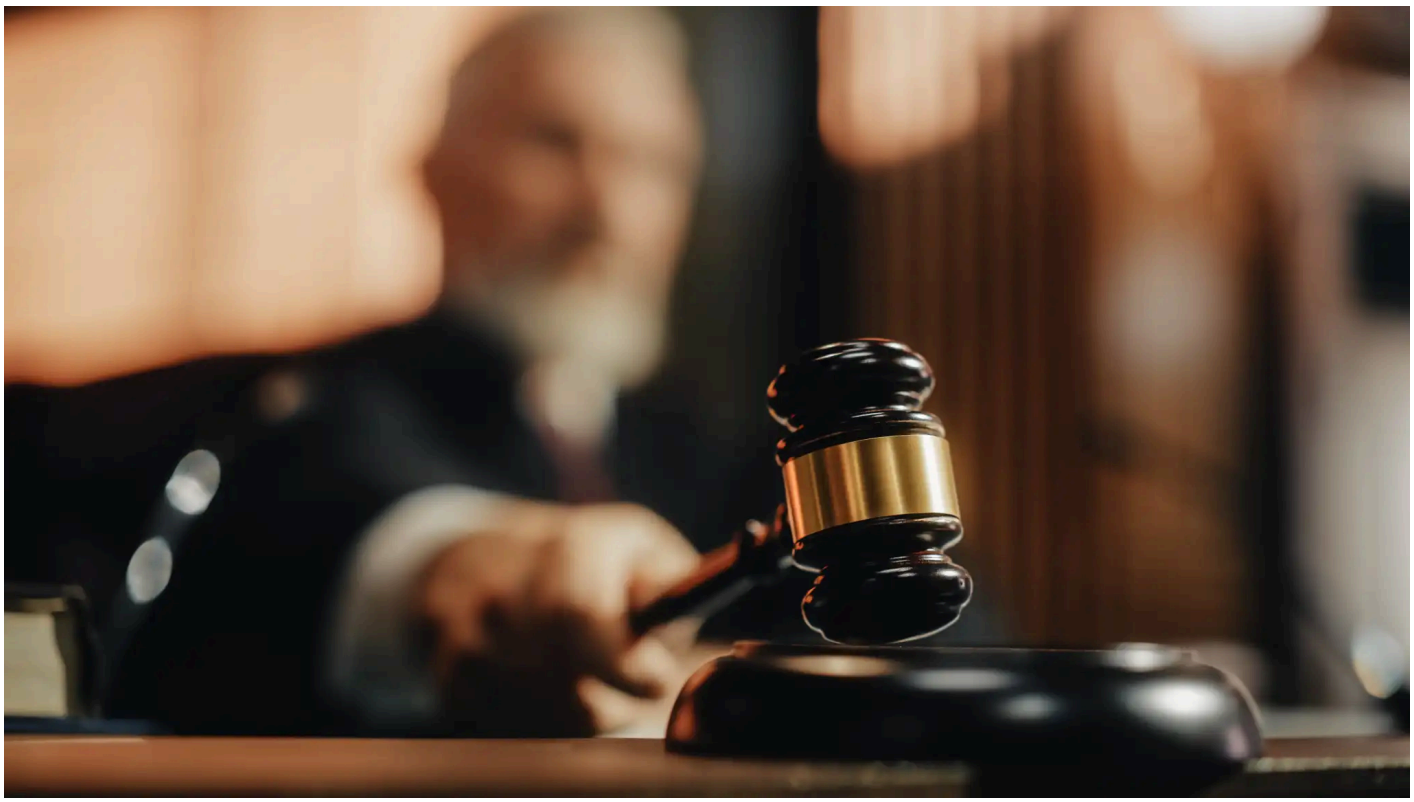
US supreme court ruling suggests change in cybersecurity disclosure process

News Analysis

Apr 16, 2024 • 6 mins

Regulation | Security

Decision puts pressure on CISOs and those crafting SEC filings as wording could be judged as "half-truths" and considered misleading.



Credit: Gorodenkoff / Shutterstock [https://enterprise.shutterstock.com/image-illustration/court-of-law-and-justice-trial-session-imparcial-honorable-judge-pronouncing-sentence-striking-gavel-focus-on-mallet-hammer-cinematic-shot-of-dramatic-not-guilty-verdict-close-up-shot-2056414424]

The United States Supreme Court unanimous ruling on an SEC disclosure case on Friday could have direct consequences on how security executives report cybersecurity incidents.

The **decision** [https://www.supremecourt.gov/opinions/23pdf/22-1165_10n2.pdf] in the Macquarie Infrastructure versus Moab Partners' case gave enterprises the green light to not report incidents that are not material, which was already directly implied **in the current SEC rules** [https://www.csoonline.com/article/1247504/how-us-sec-legal-actions-put-cisos-at-risk-and-what-to-do-about-it.html]. The court was referring to risks, specifically those that are potential and theoretical but have not necessarily happened. That might include, for example, a series of attacks overseas that could potentially be modified to hurt the company at issue. It hasn't happened yet, but it might.

The news for CISOs is that the court gave a strong caveat. It ruled that although companies are absolutely within their rights to not report such things, they have to carefully consider those items when phrasing what they *do* report to the SEC. The court warned companies that if the *unreported* information would make what the company *does* report to the SEC misleading or seriously out-of-context, the company could face serious consequences.

The Supreme Court's decision referenced such statements that would later become misleading as half-truths. "The difference between a pure omission and a half-truth is the difference between a child not telling his parents he ate a whole cake and telling them he had dessert. It requires disclosure of information necessary to ensure that statements already made are clear and complete i.e., that the dessert was, in fact, a whole cake," the Court ruled.

CISOs beware of misleading statements

Enterprises "may potentially reduce their litigation/regulatory risk by carefully crafting all affirmative statements about their cybersecurity program so that these affirmative statements are less likely to become misleading in light of future events — such as new incidents, vulnerabilities, regulations, etc. — that shareholders or regulators might allege are material," Brian Levine, managing director of cybersecurity and data privacy, strategy and transactions at EY and a former Justice Department attorney, tells CSO.

"Some companies might think that this takes the pressure off of them" but it really doesn't, Levine says. "The SEC requires companies to make so many statements about their security now that most omissions that they would make will just naturally cause some of those statements to be half-truths. Therefore, companies cannot take much solace in this decision."
If a company decides that it will not report certain information at this time, the company should do an exercise where it makes the assumption that the unannounced items do get announced. This exercise means that unannounced scenarios can't be ignored. They must be seriously considered, if for no other reason than to improve the wording of what is being announced to the SEC.

"Any disclosure is a point in time. In the (enterprise) war room examining an incident, you are always thinking about what may happen," says Justin Greis, a McKinsey partner who leads the firm's cybersecurity work in North America. The court ruled that such incidents may not have to be reported but must be examined to see if they would meaningfully color current filings.

This is why companies should then take another look at the wording of what they are about to file to the SEC and see if the unannounced item would justify wording changes to prevent it from becoming misleading.

What the Supreme Court ruling changes for CISOs

The particulars of Friday's case did not relate to cybersecurity. The case involved Macquarie Infrastructure and a securities fraud accusation because it failed to report to the SEC information about a United Nations fuel oil regulation that could have impacted the company's revenue. The UN information was already public knowledge, so it was not an issue of Macquarie hiding the information as much as it chose to not highlight it in an SEC filing. It was sued by hedge-fund manager Moab Partners.

“The question in this case is whether the failure to disclose information required by Item 303 can support a private action under Rule 10b–5(b), even if the failure does not render any statements made misleading. The Court holds that it cannot,” the ruling said. “Today, this Court confirms that the failure to disclose information required by Item 303 can support a Rule 10b–5(b) claim only if the omission renders affirmative statements made misleading.”

Friday’s Supreme Court ruling “basically says that an omission in your S-K disclosures would be actionable only if it would have countered statements you did make. So, if you don’t feel like disclosing a risk, then also avoid making affirmative statements about things that the risk would compromise,” says Chris Cronin, a security consultant who serves as an expert witness for defense, plaintiffs, and regulators. “As a shareholder, I’m not happy about the now-clear instructions for hiding risks from your 10-K. The detail and comprehensiveness of appropriate cyber risk reporting was bound to be in contention without good examples and principles to guide filers. (The ruling) only hampers a portion of the cybersecurity rule that companies seem to be pretty bad at.”

A new tabletop exercise for CISOs to consider

The ruling suggests a new modified tabletop exercise for committees deciding what should be filed following a material security incident. It should start by discussing all possible risks that the cybersecurity team anticipates in the near future and whiteboard each of them.

On another board, put the current proposed SEC filing wording for the current security incident. Then assume that each possible situation happens in the most likely manner. The team then looks back at the proposed wording and debates if any of it would appear misleading, were that potential risk to materialize.

This type of evaluation can serve as “a legal safeguard against potential claims of misleading-by-omission should other statements about the company’s security posture” change how investors might view earlier statements, says Andy Lee, who heads the privacy and data security team at the Jones Walker law firm. “Post-incident, it’s crucial for the CISO to continually review and update the disclosed information as more is learned about the incident’s scope and impact. This ongoing process helps ensure the accuracy and completeness of information in the public

domain, with the goal of preventing previously accurate statements from shading into the category of misleading as new details emerge."

Although another tabletop exercise is the last thing your teams want, Friday's Supreme Court decision may make it a worthwhile investment of time.

Sponsored Links