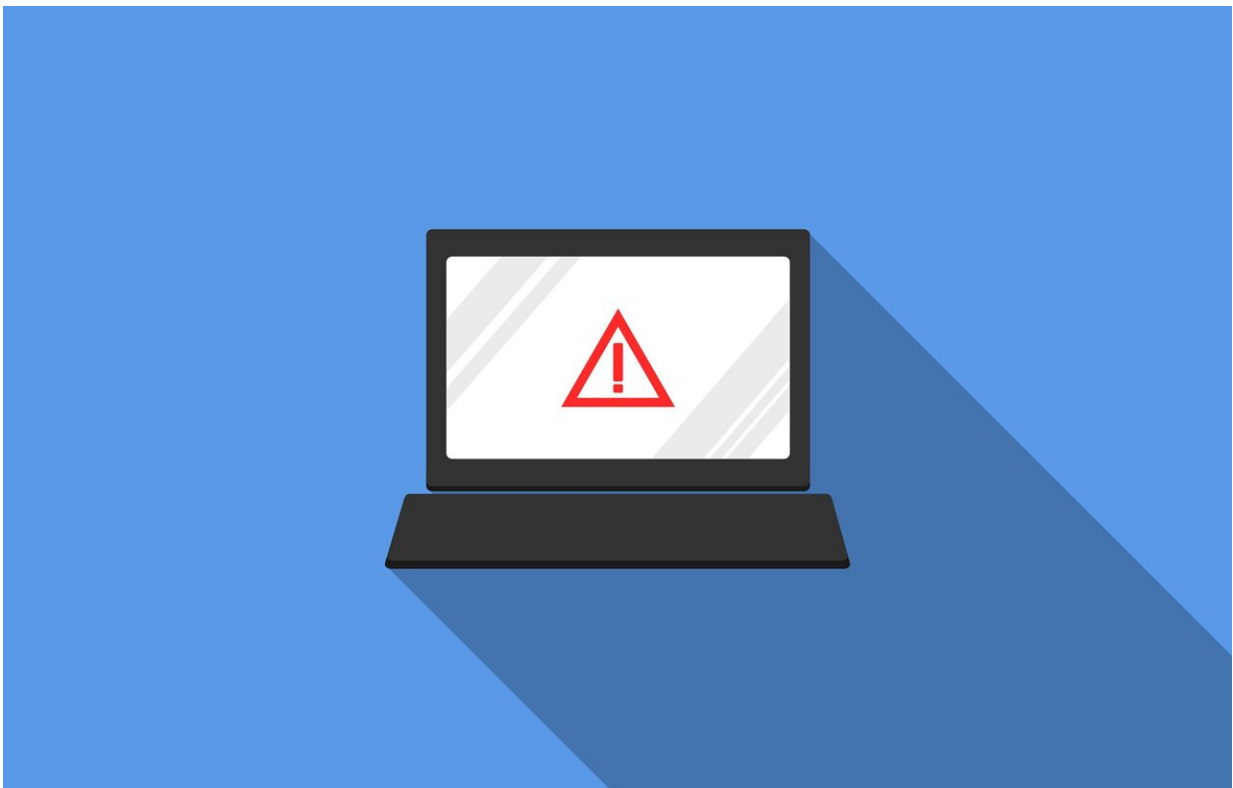


New SEC rule requires public companies to disclose cybersecurity breaches in 4 days

July 26 2023



Credit: Pixabay/CC0 Public Domain

The Securities and Exchange Commission adopted rules Wednesday to require public companies to disclose within four days all cybersecurity breaches that could affect their bottom lines. Delays will be permitted if immediate disclosure poses serious national security or public safety

risks.

[The new rules](#), passed by a 3-2 vote along party lines, also require publicly traded companies to annually disclose information on their cybersecurity risk management and executive expertise in the field. The idea is to protect investors.

Breach disclosures can be delayed if the U.S. Attorney General determines they would "pose a substantial risk to national security or public safety" and notifies the SEC in writing. Only under extraordinary circumstances could that delay be extended beyond 60 days.

"Whether a company loses a factory in a fire—or millions of files in a cybersecurity incident—it may be material to investors," SEC Chair Gary Gensler said in a statement, noting the current inconsistency in disclosures.

The rules will put "more transparency into an otherwise opaque but growing risk" and may spur improvements in cyber defenses—though potentially posing a bigger challenge for smaller companies with limited resources, Lesley Ritter, senior VP at Moody's Investors Service, said in a statement.

Technically, the clock doesn't start ticking on the four-day window for reporting until companies have determined a breach is material.

One of the dissenting Republican commissioners, Hester Peirce, [complained that](#) the new requirements overstep the SEC's authority and "seem designed to better meet the needs of would-be hackers"—who could benefit from detailed info on how companies manage cyber risk.

As well, Peirce said in a statement, the temptation for the SEC to "micromanage" company operations will only grow.

A leading figure in cybersecurity, Tenable CEO Amit Yoran, heartily welcomed the new rule.

"For a long time, the largest and most powerful U.S. companies have treated cybersecurity as a nice-to-have, not a must have. Now, it's abundantly clear that corporate leaders must elevate cybersecurity within their organizations," he said in a statement.

The rules were first proposed in March 2022, when the SEC determined that breaches of corporate networks posed an escalating risk as their digitization of operations and remote work increased—and the cost to investors from cybersecurity incidents rose.

While some critical infrastructure operators and all health care providers must by law report breaches, no federal breach disclosure law exists.

In a [new report published by IBM](#), researchers found organizations now pay an average of \$4.5 million to deal with breaches—a 15% increase over the past three years. The Ponemon Institute researchers also found that impacted businesses typically pass the costs on to consumers, who may themselves also be victims with personal information stolen in a breach.

The rule's passage also comes amid slow-moving, often cryptic disclosures—some through SEC filings—from a [major data breach](#) affecting [hundreds of organizations](#) caused by the so-called supply chain hack by Russian cybercriminals of a widely used file transfer program, MOVEit. The breach has impacted multiple universities, major pensions funds, U.S. government agencies, more than 9 million motorists in Oregon and Louisiana and companies including the BBC, British Airways, Ernst & Young and PricewaterhouseCoopers.

Many victims of the MOVEit breach were quick to point out that they

were failed by a third-party application. The new SEC rule encompasses third-party apps and notes how companies have increasingly relied on outside cloud services for data management and storage.

© 2023 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed without permission.

Citation: New SEC rule requires public companies to disclose cybersecurity breaches in 4 days (2023, July 26) retrieved 27 April 2024 from <https://techxplore.com/news/2023-07-sec-requires-companies-disclose-cybersecurity.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.