

[Articles](#)

May 04, 2022

Avoiding Data Breaches—A Guide for Boards and C-Suites

Litigation against corporate board members and C-level executives for data privacy and security claims is on the rise. Specifically, the number of suits stemming from data breaches and other cybersecurity incidents has increased as such breaches and incidents have become more common. Recently, plaintiffs have targeted corporate board members and C-level executives alleging that their data privacy–related claims result from a breach of fiduciary duties. For example, plaintiffs may allege that the board's or C-suite's breach of fiduciary duties caused or contributed to the data breach due to a failure to implement an effective system of internal controls or a failure to heed cybersecurity-associated red flags. Even if a breach does not lead to litigation or enforcement action against board members or C-level executives, data breaches can tarnish a corporation's name and lead to increased scrutiny from regulators. This year alone, the U.S. Department of Health and Human Services Office for Civil Rights has [recorded](#) over 100 breaches of unsecured electronic protected health information, or ePHI. The department noted that most cyberattacks could be prevented or substantially mitigated by implementing appropriate security measures.

[Click here to read the full article at *CPO Magazine*.](#)

Authors

Explore more in

[Privacy & Security](#)