MINTZ

Cyber Risks for the Boardroom Part 2: Why Corporate Directors Should be Concerned About Data Security Breaches

May 06, 2014 | Blog | By **Cynthia J. Larose**

VIEWPOINT TOPICS

- Privacy & Cybersecurity

RELATED PRACTICES

RELATED INDUSTRIES

All this week, we are featuring a series "Cyber Risks - Director Liability and Potential Gaps in D&O Coverage"

Part 2 of 5: Why Directors Should Be Concerned

Written by Heidi Lawson and Danny Harary

A data breach is not a unitary or self-contained event. The fallout from a breach could impact the directors as well. A security breach may lead to an investigation or an enforcement action by the Securities and Exchange Commission (SEC). The SEC may direct its investigation at the directors and subpoena the directors' documents and records. Compliance with subpoenas may be extremely expensive and, depending upon how the D&O policy defines "claim", there may not be coverage. Moreover, even if the SEC declines to investigate a data breach, the directors nevertheless face exposure to shareholder litigation and, in some cases, investigation by state authorities. Shareholder litigation in the cybersecurity context will typically allege a failure by the board to oversee and prevent the loss. This failure potentially gives rise to oversight liability under Delaware law, where many public companies are incorporated. At least two separate shareholder derivative **lawsuits** have been filed against Target's directors and officers, alleging breach of fiduciary duty, waste of corporate assets, gross mismanagement and abuse of control. A similar lawsuit was filed in 2010 against the officers and directors of **TJX Companies'** by its shareholders following a credit card data breach.

Derivative shareholder lawsuits present a large exposure to directors. Given this potential, the trend has been for directors to settle these cases, which has resulted in little guidance from the courts on director liability in the cybersecurity context. Further, there are statutory limitations on the extent to which companies may indemnify their directors for costs, awards or settlements in the derivative litigation context are generally non-indemnifiable by the company in the absence of insurance coverage. Therefore, directors can potentially face large exposures commensurate to the size of the security breach, payment for which will not be reimbursed by the company. Even if the company maintains a D&O insurance policy with adequate limits, many D&O policies contain a standard privacy exclusion (Section IV.D.), which may reduce or eliminate coverage for a cyber breach.

Tomorrow: Top Questions Directors Should be Asking About D&O Coverage

Authors

Cynthia J. Larose, Member / Co-chair, Privacy & Cybersecurity Practice

Cynthia J. Larose is Chair of the firm's Privacy & Cybersecurity Practice, a Certified Information Privacy Professional-US (CIPP-US), and a Certified Information Privacy Professional-Europe (CIPP-E). She works with clients in various industries to develop comprehensive information security programs on the front end, and provides timely counsel when it becomes necessary to respond to a data breach.