

# SEC Issues Cybersecurity Disclosure Guidance

March 31, 2018

On February 21, the SEC published interpretive "Guidance" to help public operating companies prepare disclosures about cybersecurity risks and incidents. The Guidance reinforces and expands guidance issued by the Division of Corporate Finance in 2011 regarding disclosure obligations related to cybersecurity risks and incidents. Although the new Guidance lends the Commission's imprimatur to the earlier staff guidance, two SEC commissioners took the somewhat unusual step of publishing separate statements arguing that the SEC should do more. The Guidance highlights the disclosure requirements under the federal securities laws that public operating companies must heed when considering their disclosure obligations regarding cybersecurity risks and incidents. Such disclosure requirements include those regarding the company's risk factors, description of business, legal proceedings, and financial statements, as well as management's discussion and analysis and the board of directors' role in overseeing the company risk management process. In contrast to the Division's 2011 guidance, the SEC's Guidance is notable for its emphasis on:

- the potential for selective disclosure or other misuse by insiders of cybersecurity-related material nonpublic information,
- the importance of maintaining comprehensive and effective policies and procedures governing cybersecurity-related disclosures and insider trading, and
- the role of the company's board in overseeing cybersecurity risks.

The Guidance, however, "does not address the specific implications of cybersecurity to other regulated entities under the federal securities laws, such as registered investment companies, investment advisers, brokers, dealers, exchanges, and self-regulatory organizations." Given the increasing frequency, magnitude and cost of cybersecurity incidents, some — including SEC Commissioners Jackson and Stein — believe the SEC should do more to help companies provide investors with comprehensive, particularized and meaningful disclosure about cybersecurity risks and incidents. While generally supportive of the Guidance, the separate statements issued by these

commissioners question whether it will be any more successful than the Division's 2011 guidance in eliciting more robust cybersecurity disclosures from public companies. Only time will tell.

## Authored By



Edmund J. Zaharewicz

## Related Practices

[Cybersecurity and Privacy](#)

[Financial Services Regulatory](#)

[Securities Litigation and Enforcement](#)

[Technology](#)

## Related Industries

[Life, Annuity, and Retirement Solutions](#)

[Technology](#)

©2024 Carlton Fields, P.A. Carlton Fields practices law in California through Carlton Fields, LLP. Carlton Fields publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information and educational purposes only, and should not be relied on as if it were advice about a particular fact situation. The distribution of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship with Carlton Fields. This publication may not be quoted or referred to in any other publication or proceeding without the prior written consent of the firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our Contact Us form via the link below. The views set forth herein are the personal views of the author and do not necessarily reflect those of the firm. This site may contain hypertext links to information created and maintained by other entities. Carlton Fields does not control or guarantee the accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.