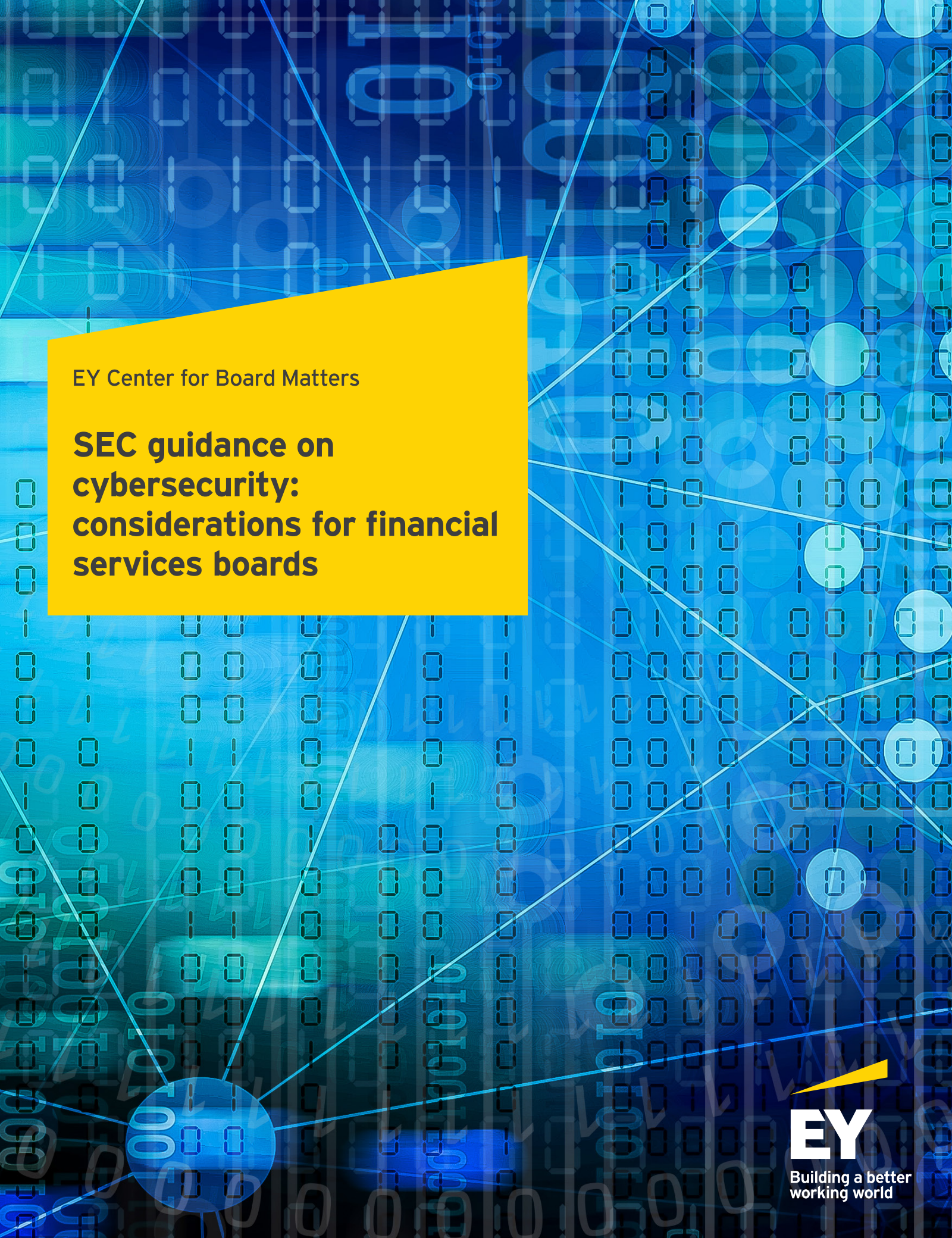


EY Center for Board Matters

SEC guidance on cybersecurity: considerations for financial services boards

EY

Building a better working world

Overview

On February 21, 2018, the Securities and Exchange Commission (SEC) unanimously approved the issuance of interpretive guidance regarding public companies' disclosure obligations under existing law regarding cybersecurity risk and incidents. This guidance is especially important given that a recent US Council of Economic Advisers report highlighted that, of more than 1,900 breaches reported in 2016, almost 25% were in the financial services industry.[1]

The SEC release updates and reinforces guidance provided in 2011 by the SEC's Division of Corporation Finance (2011 Guidance), which provided an overview of specific SEC disclosure obligations that may require companies to discuss cybersecurity risks and cyber incidents. SEC action on cybersecurity matters has been anticipated and, in a statement announcing the guidance, SEC Chair Jay Clayton noted that the SEC "will continue to evaluate developments in this area and consider feedback about whether any further guidance or rules are needed."

The new guidance carries more weight because it was issued by the SEC itself and goes beyond the 2011 Guidance by addressing the importance of insider trading prohibitions and the application of disclosure controls and procedures to cybersecurity risks and incidents, including:

- Stressing the importance of maintaining "comprehensive policies and procedures related to cybersecurity risks and incidents," in particular as incorporated into a company's disclosure controls and procedures
- Reminding companies and their directors, officers and other corporate insiders of the laws and rules relating to insider trading and selective disclosure
- Expanding the existing disclosure guidance to address how the board of directors oversees the management of cybersecurity risk, as well as management's discussion and analysis of how cybersecurity incidents affected reportable segments
- Discussing how materiality, as well as the many laws, rules, regulations and SEC form requirements, must be considered when preparing cybersecurity disclosures

[1] *The Cost of Malicious Cyber Activity to the U.S. Economy* (page 19), The Council of Economic Advisers, February 2018.

Board considerations

"Cybersecurity risks pose grave threats to our investors, our capital markets, and our country," states the SEC in the release. It continues: "[a]s companies' exposure to and reliance on networked systems and the Internet have increased, the attendant risks and frequency of cybersecurity incidents also have increased. … Given the frequency, magnitude and cost of cybersecurity incidents, the Commission believes that it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack."

We observed in our *Top priorities for US Boards in 2018* that cybersecurity, along with other technology matters, is a key priority for board focus. Boards need to be aware of the SEC's new guidance as they continue to manage and enhance their oversight of cybersecurity risks and incidents, as well as company policies and procedures that should specifically address these matters. Financial services boards have a critical role to play in governing cyber risks and have a number of competing issues to grapple with in order to provide effective oversight.[2]

Policies and procedures

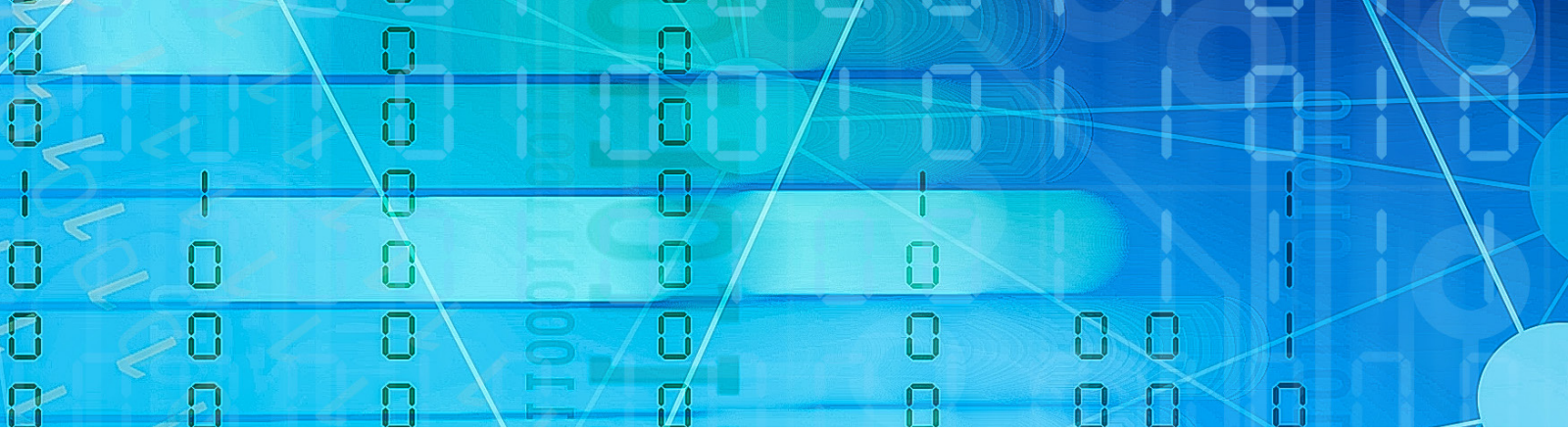
Disclosure controls and procedures

The release states that "[c]rucial to a public company's ability to make any required disclosure of cybersecurity risks and incidents in the appropriate timeframe are disclosure controls and procedures that provide an appropriate method of discerning the impact that [cybersecurity risks and incidents] may have on the company and its business, financial condition, and results of operations, as well as a protocol to determine the potential materiality of such risks and incidents."

The release adds that effective disclosure controls and procedures are "best achieved when a company's directors, officers, and other persons responsible for developing and overseeing such controls and procedures are informed about the cybersecurity risks and incidents that the company has faced or is likely to face."

Disclosure controls and procedures, therefore, should provide an "early warning system" to enable companies to determine whether — with respect to any matter, including a cybersecurity matter — they need to file a current report on Form 8-K, make a disclosure in any other SEC filing, issue a press release or suspend trading in its stock. Disclosure controls and procedures should provide for a clear line of vertical organizational reporting up the chain to senior management of any matter that could implicate disclosure, compliance or any other important business matters.

[2] *Governing cyber risk in financial services*, EYGM Limited, August 2017.



Boards should discuss with management whether their companies' disclosure controls and procedures are appropriately designed to capture and address cybersecurity matters, including to help confirm that relevant information about cybersecurity risks and incidents is accumulated and communicated to senior management and the board to allow timely decisions about what disclosure may be appropriate or required under the circumstances.

Codes of ethics and insider trading policies

The release reminds companies that information about cybersecurity risks and incidents may be material nonpublic information. As such, the SEC encourages companies to consider how their codes of ethics and insider trading policies take into account and look to prevent trading on the basis of material nonpublic information regarding cybersecurity risks and incidents.

Significantly, the SEC states "that companies would be well served by considering how to avoid the appearance of improper trading during the period following an incident and prior to the dissemination of disclosure."

Boards, or the appropriate board committee, should discuss with management whether the company's insider trading policy and code of ethics adequately explain that cybersecurity matters may be material and thus required to be disclosed, and that, prior to disclosure of material information about an existing cybersecurity matter, prohibitions will be imposed on trading in the company's securities. Revisions to insider trading policies and codes of ethics may be appropriate. In particular, in view of the SEC's statement regarding avoiding the appearance of improper trading, careful consideration should be given to policies and procedures regarding trading windows and blackout periods, and possibly on Rule 10b5-1 trading programs and plans.

Regulation FD policies

The release reminds companies that Regulation FD (Fair Disclosure) prohibits companies and persons acting on their behalf (often noted as "authorized spokespersons" in a company's Regulation FD policy) from selectively disclosing material nonpublic information about cybersecurity risks and incidents to Regulation FD enumerated persons.

Boards should discuss with management whether the company's Regulation FD policy specifically identifies cybersecurity risks and incidents as potentially being material nonpublic information subject to the policy.

Board risk oversight

The release reiterates a prior SEC statement that "disclosure about the board's involvement in the oversight of the risk management process should provide important information to investors about how a company perceives the role of its board and the relationship between the board and senior management in managing the material risks facing the company." In this regard, the SEC states that companies "must [disclose] how the board administers its risk oversight function." The release further provides that companies should disclose:

- The company's cybersecurity risk management program
- The board's role in overseeing the management of material cybersecurity risks
- How the board engages with management on cybersecurity issues

Financial services firms have been investing heavily in cyber risk management in recent years, particularly in how well it is operating across the three lines of defense: first line (business units, including technology), second line (risk and compliance) and third line (internal audit).[3] Boards of those firms have an important role to play in overseeing those investments, and more broadly in validating that their firms are sufficiently resilient in the context of cyber risks.[4]

To address this guidance, boards should review their meeting calendars and agendas to determine whether they permit adequate frequency and sufficient time as well as information that is appropriate to oversee cybersecurity risks and discuss cybersecurity matters with management, including how cybersecurity risks are identified and assessed in light of ongoing and increasingly complex cybersecurity threats. With risk and compliance getting more involved in cybersecurity, as well as internal audit and technology, it is important that financial services firms' audit and risk committees — and board technology committees, where they exist — determine how best to engage all these functions effectively in governing cybersecurity.

> ***"I urge public companies to examine their controls and procedures, with not only their securities law disclosure obligations in mind, but also reputational considerations around sales of securities by executives."*** — SEC Chairman Jay Clayton

Boards should also discuss with management whether the company's enterprise risk management program and disclosure controls and procedures are appropriately interlinked, scaled and flexible to serve their purposes with respect to identification, handling and disclosure of cybersecurity risks and incidents. The manner in which cyber risk is mitigated through cyber insurance is also important.

[3] *Cyber risk management across the lines of defense*, EYGM Limited, April 2017.
[4] *Cyber resiliency: evidencing a well-thought-out strategy*, EYGM Limited, August 2017.

Disclosures

The release updates and reinforces the 2011 Guidance by reminding companies that the SEC's disclosure requirements apply to cybersecurity risks and incidents that could have a material impact on the company, including:

- Risk factors
- Management's discussion and analysis of financial condition and results of operations
- Business description
- Legal proceedings
- Financial statement disclosures

The SEC expects companies to disclose material cybersecurity risks and incidents that are material to investors, including the financial, legal or reputational consequences. In this regard, the SEC also reiterates that companies are not expected to "publicly disclose specific, technical information about their cybersecurity systems, the related networks and devices, or potential system vulnerabilities in such detail as would make such systems, networks, and devices more susceptible to a cybersecurity incident," or other details that would provide a road map for anyone seeking to penetrate a company's security protections.

The SEC will continue to monitor cybersecurity disclosures carefully and consider whether additional actions are needed. The guidance became effective on February 26, 2018, upon publication in the Federal Register.[5]

For more cyber and privacy insights, visit ey.com/fsGDPR or ey.com/fscyber

[5] *Commission Statement and Guidance on Public Company Cybersecurity Disclosures,* Federal Register, February 26, 2018.

Questions for the board to consider

- Do the company's disclosure controls and procedures provide an "early warning system" that enables the company to identify, assess, address and make timely disclosures about cybersecurity risks and incidents?
- Do the company's disclosure controls and procedures, or other relevant policies and procedures, include escalation criteria and protocols that facilitate timely communications to the board on cybersecurity-related risk events or incidents?
- Has the board considered an independent assessment of the company's cybersecurity risk management process and related reporting to help cofirm that the processes are appropriate and sound?
- Do the company's code of ethics, Regulation FD policy, insider trading policy and procedures for determining trading windows and blackout periods appropriately and clearly address cybersecurity risks and incidents? If a cybersecurity risk or incident occurred, can management determine whether or when to prohibit trading in the company's securities or to prevent authorized spokespersons from selectively disclosing information?
- Does the board understand how the cybersecurity risk management program is integrated into the company's overall enterprise risk management program, and are the reporting lines for compliance personnel (e.g., Chief Information Security Officer) who have responsibility for cybersecurity risk oversight appropriate?
- Does the board have the right directors, committee structure and access to information to oversee cybersecurity matters? Has the company considered whether it should enhance its disclosures about how cybersecurity fits into the board's risk oversight function and how the board is engaging with management on this issue?
- Does the company provide appropriate disclosures about cybersecurity risks and incidents consistent with the new guidance?

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

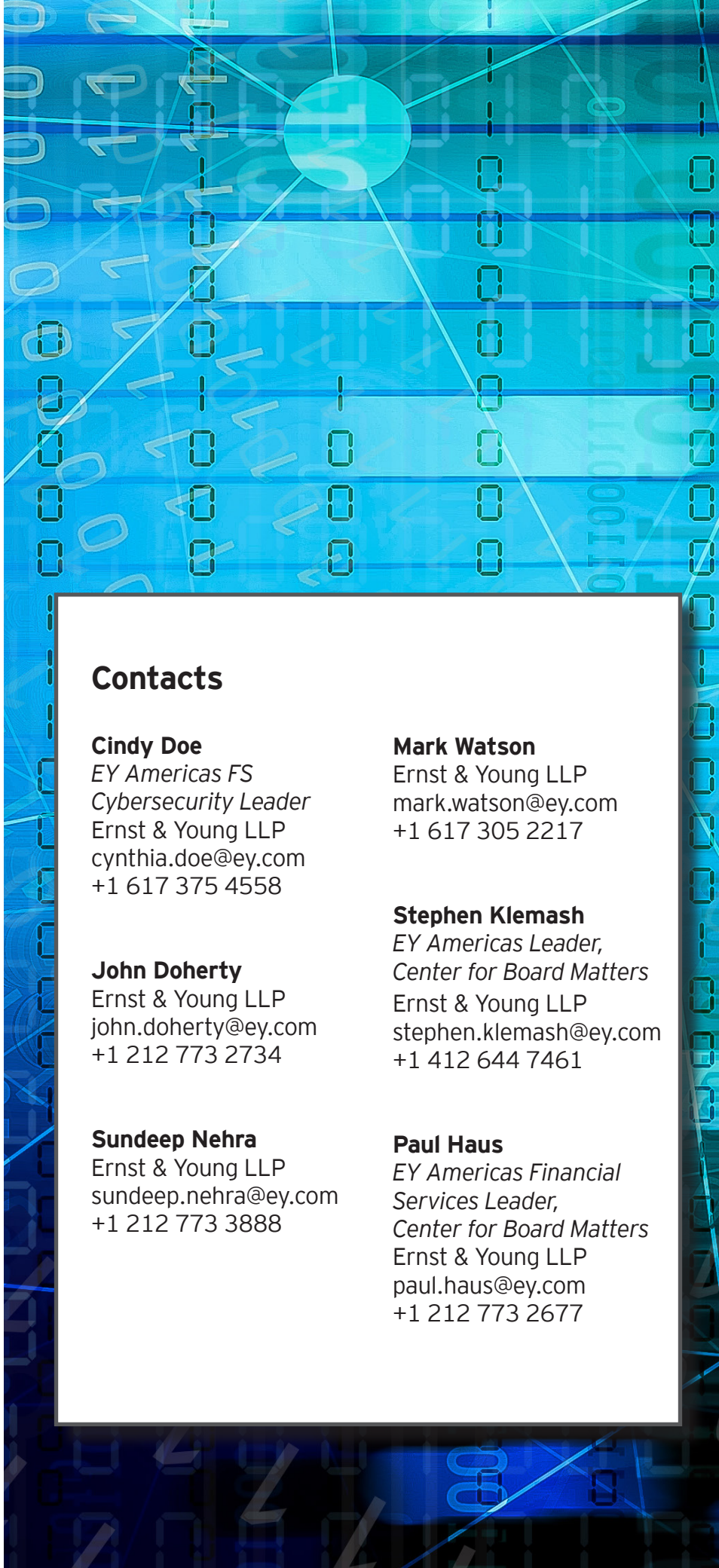
Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

About the EY Center for Board Matters
Effective corporate governance is an important element in building a better working world. The EY Center for Board Matters supports boards, committees and directors in their oversight role by providing content, insights and education to help them address complex boardroom issues. Using our professional competencies, relationships and proprietary corporate governance database, we are able to identify trends and emerging governance issues. This allows us to deliver timely and balanced insights, data-rich content, and practical tools and analysis for directors, institutional investors and other governance stakeholders.

US SCORE no. 01832-181US

CSG no. 1803-2616692

ED None



Contacts

Cindy Doe
EY Americas FS Cybersecurity Leader
Ernst & Young LLP
cynthia.doe@ey.com
+1 617 375 4558

John Doherty
Ernst & Young LLP
john.doherty@ey.com
+1 212 773 2734

Sundeep Nehra
Ernst & Young LLP
sundeep.nehra@ey.com
+1 212 773 3888

Mark Watson
Ernst & Young LLP
mark.watson@ey.com
+1 617 305 2217

Stephen Klemash
EY Americas Leader, Center for Board Matters
Ernst & Young LLP
stephen.klemash@ey.com
+1 412 644 7461

Paul Haus
EY Americas Financial Services Leader, Center for Board Matters
Ernst & Young LLP
paul.haus@ey.com
+1 212 773 2677