SEC Adopts Cybersecurity Disclosure Rules for Public Companies

On July 26, 2023, in a 3-2 vote, the Securities and Exchange Commission (the "SEC" or the "Commission") adopted final rules regarding disclosure by public companies, including foreign private issuers ("FPIs"), of cybersecurity risk management, strategy, governance and related incidents (the "Final Rules"). In particular, the Final Rules require: (i) current reporting of material cybersecurity incidents; and (ii) annual reporting of companies' processes to identify, assess and manage cybersecurity risks, as well as management's role in assessing and managing, and the board's role in overseeing, such risks. In doing so, the Final Rules will significantly expand public companies' reporting obligations with respect to cybersecurity matters. The Final Rules will go into effect 30 days after publication in the Federal Register and include a short runway for compliance in, generally, December 2023.

BACKGROUND

Over the past 12 years, both the Commission and its staff have issued interpretive guidance concerning the application of existing disclosure requirements to cybersecurity risks and incidents. In 2011, the Division of Corporation Finance issued interpretive guidance (the "2011 Staff Guidance"), which provided its views about the applicability of existing SEC disclosure requirements to cybersecurity matters. In 2018, the Commission issued its own interpretive guidance (the "2018 Commission Guidance"), reinforcing and expanding on the 2011 Staff Guidance and explaining that public companies should consider the materiality of cybersecurity risks and incidents when preparing disclosure in their registration statements and periodic and current reports.

Building on this guidance, the Commission proposed new cybersecurity disclosure rules (the "Proposal") on March 9, 2022, and the Final Rules generally track the Proposal with some key exceptions noted below. In issuing the Proposal and adopting the Final Rules, the Commission highlighted, among other factors, the increasing frequency and severity of cyberattacks on public companies, the widespread reliance on third-party providers of information technology services ("IT service providers"), the continued prevalence of remote work arrangements and investors' perception of a current lack of consistency across public companies' disclosures regarding cybersecurity matters.

NEW CURRENT REPORTING REQUIREMENTS

The Final Rules add a new Item 1.05 to Form 8-K requiring disclosure of any cybersecurity incident a company experiences that it determines to be material, including the material aspects of the incident's nature, scope and timing and its impact or reasonably likely impact on the company's business, financial condition and results of operations. These requirements, which are narrower than those contained in the Proposal, are intended to focus "on an incident's basic identifying details and its material impact or reasonably likely material impact" rather than granular details about the incident, the disclosure of which, commenters pointed out, could create additional risks for companies.

The foregoing information must be filed under Item 1.05 of Form 8-K within four business days of the company determining that the incident was material (rather than the date the incident occurred or was discovered). The materiality determination must be made "without unreasonable delay"; the Commission had proposed, but ultimately decided against, a stricter standard of "as soon as reasonably practicable". This change was intended to avoid the creation of "undue pressure to make a materiality determination before a registrant has sufficient information to do so". Late filing of an Item 1.05 Form 8-K will not result in the loss of Form S-3 eligibility. Information on Item 1.05 will be considered filed, not furnished.

In response to commenters' concerns, the Commission explicitly included in an instruction to Item 1.05 the clarification that a company "need not disclose specific or technical information about its planned response to the incident or its cybersecurity systems, related networks and devices, or potential system vulnerabilities in such detail as would impede the registrant's response or remediation of the incident". The Commission also omitted the requirement from the Proposal to disclose remediation status, whether the incident is ongoing or whether data was compromised (although the latter should factor into companies' materiality analyses).

Exceptions

Notably, the Commission included in Item 1.05 a provision that allows for delays in filing the Form 8-K if the United States Attorney General determines that the disclosure "poses a substantial risk to national security or public safety" and notifies the Commission of such determination in writing. Under this exception, the filing may be initially delayed up to 30 days following the date when the disclosure was originally due. The Attorney General may grant an additional 30-day extension if he or she determines that the disclosure continues to pose such a substantial risk. In "extraordinary circumstances", the disclosure may be delayed for up to 60 more days, but only if the disclosure continues to pose a threat to national security (*i.e.*, not just to public safety, which the Commission views as less critical). Finally, if the Attorney General indicates that further delay is necessary, the Commission will consider additional delays and may grant them through exemptive order.

In terms of process, the Commission has indicated that it has worked with the Department of Justice (the "DOJ") to set up an interagency communication system to allow for the Attorney General's determinations to be provided to the Commission in a timely manner. The Commission also stated that the DOJ will alert companies that the required notification "to the Commission has been made, so that the registrant may delay filing its Form 8-K", suggesting that submission of such notification is necessary to permit such delay under the rule. If so, this will create pressure on companies to establish and maintain clear lines of communication with DOJ officials to avoid missing the filing deadline while waiting for approval.

In adopting the Final Rules, the Commission also noted that the Attorney General "may take into consideration other Federal or other law enforcement agencies' findings" in determining whether to make an exception, and that other agencies may request that the Attorney General grant an exception. This would appear to be particularly important in the context of incidents posing a risk to public safety, which are less likely than incidents posing a risk to national security to involve the DOJ in the first place. Companies will be watching closely to see if the Commission or DOJ publishes guidance or an FAQ that addresses how companies should navigate this interagency process.

Despite receiving significant support for the idea from commenters, the Commission did not adopt a general provision for delays pending law enforcement investigations. Nor did the Commission generally agree with the concern voiced by commenters that the requirements of Form 8-K Item 1.05 would conflict with various federal and state breach notification laws and regulations, such as the rules issued by the Federal Trade Commission and federal banking regulators, as well as forthcoming regulations expected from the Cybersecurity & Infrastructure Security Agency pursuant to the Cyber Incident Reporting for Critical Infrastructure Act of 2022. While the Commission did identify one such conflict and adopt an exception for companies that are subject to the Federal Communications Commission's notification rule for breaches of customer proprietary network information, which applies specifically to telecommunications providers, it otherwise concluded that "Item 1.05 neither directly conflicts with nor impedes the purposes of other such laws and regulations".

Accordingly, apart from the limited exceptions noted above, once a company determines that an incident is material, it must disclose the incident under Item 1.05 of Form 8-K within four business days, regardless of whether remediation is continuing or it would otherwise benefit from additional time prior to disclosure. At the same time, a company that makes a disclosure under Item 1.05 will also need to carefully coordinate that disclosure with any other breach reporting regimes to which it may be subject.

Amendments

If any information required by Form 8-K Item 1.05 is not determined or is unavailable when the initial filing is due (*e.g.*, with respect to the incident's scope or impact), companies must include a statement to that effect in the initial filing and amend such filing to provide the new information within four business days after (i) making such determination (without unreasonable delay) or (ii) such information becomes available. This requirement was added in lieu of Item 106(d)(1) in the Proposal, which would have required inclusion of updates concerning prior cybersecurity incidents in periodic reports; instead, all reporting of material cybersecurity incidents will be found only in current reports under the Final Rules. Importantly, the Final Rules only require updates for previously undetermined or unavailable information, not all new information (although, of course, a company continues to have a duty to correct a prior disclosure if it determines the disclosure was untrue or materially misleading when made).

Third-Party Information

As noted below, given the operative definitions in the Final Rules, a cyberattack on a company's IT service provider may trigger disclosure by the company under Item 1.05 of Form 8-K. However, the Commission chose not to provide any accommodations for companies' disclosure of information from IT service providers. Commenters made a number of suggestions in light of the fact that companies have relatively little control over the behavior of their IT service providers, including not requiring disclosure of incidents at IT service providers at all, provision of a safe harbor for such disclosure and a longer reporting timeframe. In rejecting these suggestions, the Commission reasoned that "whether an incident is material is not contingent on where the relevant electronic systems reside or who owns them". Put differently, the Commission did "not believe a reasonable investor would view a significant breach of a registrant's data as immaterial merely because the data were housed on a third-party system, especially as companies increasingly rely on third-party cloud services that may place their data out of their immediate control".

Materiality

To conduct materiality analyses for purposes of Item 1.05 of Form 8-K, companies are instructed to use the traditional definition of materiality as articulated by the Supreme Court and endorsed consistently by the Commission—namely, that information is material if there is a substantial likelihood that (i) a reasonable investor would consider the information important in making a buy, sell or hold investment decision or a voting decision or (ii) disclosure of such information would have been viewed by a reasonable investor as having significantly altered the "total mix" of information available. Consistent with prior guidance on materiality, the Commission noted that "'[d]oubts as to the critical nature' of the relevant information should be 'resolved in favor of those the statute is designed to protect,' namely investors".

In discussing materiality under Item 1.05, the Commission stated: "By way of illustration, harm to a company's reputation, customer or vendor relationships, or competitiveness may be examples of a material impact on the company. Similarly, the possibility of litigation or regulatory investigations or actions, including regulatory actions by state and Federal governmental authorities and non-U.S. authorities, may constitute a reasonably likely material impact on the registrant". The Commission specifically declined to adopt a quantifiable trigger for Item 1.05 "because some cybersecurity incidents may be material yet not cross a particular financial threshold". For instance, the Commission explained that while "a cybersecurity incident that results in the theft of information may not be deemed material based on quantitative financial measures alone, it may in fact be material given the impact to the registrant that results from the scope or nature of harm to individuals, customers, or others". Needless to say, making materiality determinations that are both credible and efficient will be one of the most important—and challenging—aspects of complying with the Final Rules.

Definitions

The Final Rules contain important new definitions as well. "Cybersecurity incident" is defined as "an unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein". This definition was revised in the Final Rules to specifically address a series of related attacks that may be material in the aggregate even if each individual attack may be immaterial when viewed in isolation. The Commission accordingly dropped Item 106(d)(2) from the Proposal, which would have required disclosure when a series of previously undisclosed attacks—even if unrelated—becomes material when taken as a whole. Under the definition in the Final Rules, companies analyzing the materiality of an individual cybersecurity incident should be mindful of the importance of looking back at any potentially related or similar incidents.

"Information systems" means "electronic information resources, owned or used by the registrant, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the registrant's information to maintain or support the registrant's operations". Notably, the phrase "or used by" picks up the operations and infrastructure of IT service providers such as cloud service providers, meaning an attack on a company's IT service provider could trigger an Item 1.05 Form 8-K for a public company.

NEW ANNUAL REPORTING REQUIREMENTS

The Commission also adopted new requirements applicable to public companies' annual reports on Form 10-K (not quarterly reports or proxy statements) in Item 106 of Regulation S-K. Under Item 106(b), public companies must describe their processes, if any, for assessing, identifying and managing material risks from cybersecurity threats, including, but not limited to: (i) whether and how any such processes have been integrated into their overall risk management systems; (ii) whether they engage assessors, consultants, auditors or other third parties in connection therewith; and (iii) whether they have processes to oversee and identify risks to the company associated with their use of IT service providers.

In addition, companies must describe whether and how any risks from cybersecurity threats, including as a result of previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect their business strategy, results of operations or financial condition. With respect to this requirement, the Commission specifically cautioned that "registrants should consider whether they need to revisit or refresh previous disclosure, including during the process of investigating a cybersecurity incident". Moreover, this requirement is distinct from the new Form 8-K requirement to disclose material cybersecurity incidents on an ongoing basis, focusing instead on the impact of *risks* from cybersecurity threats on a forward-looking basis.

Under Item 106(c), companies must also describe the board's oversight of risks posed by cybersecurity threats and, if applicable, identify any board committee or subcommittee responsible for the oversight of such risks and describe the processes by which the board (or relevant committee) is informed about such risks. Notably, the Commission did not adopt Item 407(j) from the Proposal, which received significant pushback and would have required disclosure about the cybersecurity expertise of individual board members. The requirement from the Proposal to disclose the frequency of board or committee discussions regarding cybersecurity was also eliminated.

Further, companies must describe management's role in assessing and managing material risks posed by cybersecurity threats, including (i) whether and which management positions or committees are responsible for assessing and managing such risks and the relevant expertise of their current occupants or members; (ii) the processes by which management is informed about, and monitors the prevention, detection, mitigation and remediation of, cybersecurity incidents; and (iii) whether management reports information about such risks to the board or a committee or subcommittee of the board. Note that, while the requirements regarding management's role are significantly more detailed than those concerning the board, they only apply to management of *material* cybersecurity risks, whereas the board requirements apply to cybersecurity risks generally. The requirement to disclose management expertise also distinguishes cybersecurity from other key risk areas, regarding which management expertise is not required to be disclosed under SEC rules.

Finally, while the Commission did not extend Item 106 to registration statements, it did reiterate its view from the 2018 Commission Guidance that "[c]ompanies should consider the materiality of cybersecurity risks and incidents when preparing the disclosure that is required in registration statements".

APPLICABILITY TO OTHER ISSUERS

The Final Rules also apply to FPIs, though with some differences. Form 6-K has been amended to expressly add "material cybersecurity incidents" to the indicative list of events that FPIs may need to report if such incidents constitute information that they (i) make or are required to make public or otherwise disclose pursuant to the laws of their home jurisdictions, (ii) file or are required to file with any stock exchange on which their securities are traded (and which is made public by that exchange) or (iii) distribute or are required to distribute to their security holders. These criteria are the existing requirements that govern when FPIs need to furnish a Form 6-K, which remain unchanged by the Final Rules. And, in their annual reports on Form 20-F, FPIs must provide the same disclosure required by Item 106 under new Item 16K.

The Commission did not amend Form 40-F, instead continuing to rely on the multijurisdictional disclosure system whereby eligible Canadian FPIs use Canadian disclosure standards and documents to satisfy SEC registration and disclosure requirements.

Smaller reporting companies ultimately were not exempted from the Final Rules but were given more time to comply with the current reporting requirements of Forms 8-K and 6-K (as explained below).

Asset-backed securities issuers are exempted from the Final Rules.

COMPLIANCE DATES

The Commission provided a surprisingly short runway for compliance with the Final Rules. With respect to the current reporting requirements on Forms 8-K and 6-K, all companies other than smaller reporting companies must begin complying on the later of 90 days after the date of publication in the Federal Register or December 18, 2023. Smaller reporting companies will have an additional 180 days and therefore must begin complying with the current reporting requirements on the later of 270 days after the date of publication in the Federal Register or June 15, 2024.

Regarding the annual reporting requirements on Forms 10-K and 20-F, all companies must begin providing the applicable disclosures in annual reports for fiscal years ending on or after December 15, 2023.

The rapid timing for compliance with the Final Rules may be a harbinger of the Commission's expectations for future rule adoptions.

NEXT STEPS

Cybersecurity disclosure was already a focus area for the Commission and its staff, including the Division of Enforcement, before adoption of the Final Rules. Now that the Final Rules have been adopted, companies should carefully evaluate their existing cybersecurity policies and procedures against the backdrop of the Final Rules and the new disclosures that will be required. This evaluation should address board and management oversight of cybersecurity, including structural elements (*e.g.*, board and management committees, management positions and use of outside consultants and other experts), as well as existing cybersecurity infrastructure; incident response training; internal incident escalation and reporting; and overall preparedness. Companies should also assess the integration of each of these items with their disclosure controls and procedures

("DCP") and, as appropriate, their internal control over financial reporting.

Companies should specifically consider whether changes to their DCP are advisable or appropriate to ensure compliance with the new Form 8-K requirements, including to ensure that their DCP is designed to facilitate analysis of cybersecurity incidents after learning of an incident. Relatedly, companies should revisit the materiality framework (including specific analytical criteria) applicable to cybersecurity incidents, including in consultation with outside counsel or other experts to the extent possible.

As part of their evaluation of their incident response training, companies should review their existing contacts with the DOJ and other relevant law enforcement agencies, given the Form 8-K Item 1.05 delay provision described above.

In addition, in light of the fact that an attack on a company's IT service provider may trigger an Item 1.05 Form 8-K requirement for the company, public companies also should evaluate their policies and procedures with respect to, and agreements with, their IT service providers to make sure they have adequate and timely access to information. As noted above, the Commission considered but did not adopt a safe harbor for information disclosed about third-party systems.

Companies should also begin thinking about what their updated annual disclosures will look like, starting with a review of their existing cybersecurity disclosures. Steps that companies take now to prepare for the new Form 8-K reporting requirements (such as enhancements to DCP, including robust reporting lines and supervision of materiality determinations and related disclosures) will contribute to robust subsequent annual disclosures, since Item 106 and Item 16K focus on companies' risk management, strategy and governance.

NEW YORK

John W. White
+1-212-474-1732
jwhite@cravath.com

John D. Buretta
+1-212-474-1260
jburetta@cravath.com

Benjamin Gruenstein
+1-212-474-1080
bgruenstein@cravath.com

Evan Norris
+1-212-474-1524
enorris@cravath.com

Michael L. Arnold
+1-212-474-1664
marnold@cravath.com

Kimberley S. Drexler
+1-212-474-1434
kdrexler@cravath.com

WASHINGTON, D.C.

Elad L. Roisman
+1-202-869-7720
eroisman@cravath.com

Jeffrey A. Rosen
+1-202-869-7724
jrosen@cravath.com

CRAVATH, SWAINE & MOORE LLP

NEW YORK

Worldwide Plaza
825 Eighth Avenue
New York, NY 10019-7475
+1-212-474-1000

LONDON

CityPoint
One Ropemaker Street
London EC2Y 9HR
+44-20-7453-1000

WASHINGTON, D.C.

1601 K Street NW
Washington, D.C. 20006-1682
+1-202-869-7700

cravath.com