SEC APPROVES NEW CYBERSECURITY DISCLOSURE RULES, INCLUDING REPORTING OF MATERIAL INCIDENTS WITHIN FOUR BUSINESS DAYS

On Wednesday, the SEC adopted new disclosure rules to enhance and standardize corporate disclosure regarding cybersecurity risk management, strategy and governance, as well as regarding cybersecurity incidents. The new rules were proposed in March 2022 (*see* my previous briefing note, available here),[1] and follow interpretive SEC staff guidance issued in 2011 and SEC interpretive guidance issued in 2018, which reinforced and expanded upon the 2011 staff guidance. Incidentally, the SEC confirms that the 2011 and 2018 interpretive guidance remains in place, as the prior guidance covers a number of topics not addressed by the new rules, and also notes that certain elements of the new rules reinforce the prior guidance.

The new rules were prompted by the SEC's perception that, despite the prior guidance, registrants' cybersecurity disclosure was not as robust as expected, investors need more timely and more consistent disclosure, and legislative and regulatory developments in 2022 (namely, the Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA"), the regulations for which have yet to be issued by the Cybersecurity & Infrastructure Security Agency ("CISA"),[2] and the Quantum Computing Cybersecurity Preparedness Act) will not provide the level of public cybersecurity disclosure needed by investors in public companies.

In short, the new rules supplement the 2011 and 2018 guidance, by adding for both domestic registrants and foreign private issuers affirmative disclosure obligations regarding cybersecurity incidents and by centralizing cybersecurity strategy, risk management and governance disclosures. A "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."

The new rules are effective 30 days after publication in the *Federal Register*. Risk management and governance disclosure will be required in Form 10-K or 20-F annual reports filed for fiscal years beginning on or after December 15, 2023. Cybersecurity incident disclosure requirements apply, other than for smaller reporting companies, on the later of 90 days after publication in the *Federal Register* and December 18, 2023. Smaller reporting companies have an additional 180 days from the later of 270 days after publication in the *Federal Register* and June 15, 2024.

Among the key takeaways: domestic registrants will have four business days after a cybersecurity incident is determined to be material to report it on a Form 8-K. Foreign private issuers will be subject to Form 6-K disclosure if the predicates are met. Domestic and foreign private issuers will have annual reporting requirements in respect of risk management and governance around cybersecurity.

---

[1] The initial public comment period closed in May 2022, but was reopened in February of this year.

[2] The CIRCIA will require "covered entities" (entities in the critical infrastructure sector, satisfying the definition to be established by the CISA Director in a final rule) to report "covered cyber incidents" (also to be defined) to CISA within 72 hours.

Background

Cyber risks are surging and, not surprisingly, cybersecurity frequently is cited at the top of the list of threats confronting businesses. In today's digital world, every business (and, in fact, every individual) is a potential target of a cybersecurity attack, and every business therefore faces potential operational, brand, reputational, legal, regulatory and financial risks. Those financial risks can include business interruption costs, lost revenue, ransom payments, remediation costs, indemnity payments, protections costs, liability costs and lost assets.

Every day, more cyber-attack surfaces and vectors come online. Increased reliance on third-party service providers for IT services and the pervasive embrace of remote work have already been shown to increase vectors of vulnerabilities, and the Metaverse will introduce new vectors of vulnerabilities. Generative AI will significantly exacerbate vulnerabilities (both in terms of new malign tools that can be deployed at scale for nominal costs and the potential for deepfakes).

Malign foreign actors are more active, whether to steal IP, for financial gain or to threaten critical infrastructure, among other drivers. Geopolitical tensions generally are elevating cybersecurity threats.

Citing the proposing release, Commissioner Jaime Lizárraga noted that, over the past decade, cybersecurity incidents have increased six-fold; last year, 83% of business organizations experienced more than one data breach; and, overall, some estimates of the economy-wide total costs of cybersecurity incidents run as high as trillions of dollars per year in the United States, alone. The SEC cited a study by Cyentia Institute and SecurityScorecard that found that 98% of organizations use at least one third-party vendor that has experienced a breach in the past two years. IBM estimates that 82% of breaches involved data stored in the cloud – public, private or, in 39% of the cases, multiple environments.

Ransomware attacks in 2022 are estimated to have increased 13% last year over the prior year, which is equivalent to the total for the preceding five years. According to statistics collected by astra, in 2022, there were an average of 2,000 cyberattacks per day and 300,000 new malware are created every day, 92% of which are delivered via email and have a detection period of 49 days. An estimated 4.1 million websites have malware at any given time. In the first half of 2022, there were 2.8 billion malware attacks, not counting over 5 million mobile malware, adware and riskware attacks that were blocked in Q2 of 2022, alone.

Statista estimates that 71% of businesses worldwide were victims of ransomware attacks in 2022, up from 55.1% in 2018. Statista estimates that the average cost of a data breach in the United States was $9.4 million in 2022 (up from $5.5 million in 2012). According to IBM based on research by the Ponemon Institute, the average cost of a data breach globally is $4.45 million (up from $3.86 million in 2020).

Arctic Wolf estimates that during the second quarter of 2022, there was a significant increase in business email compromise (ransomware) attacks, driven in part by human error, but 80% are driven by exploitation of unpatched vulnerabilities and remote access tools.

Looking ahead, according to a Deloitte Center for Controllership poll, 48.8% of C-suite executives and other senior executives expect the number and size of cybersecurity incidents targeting their enterprises' accounting and financial data to increase in 2023, yet only 20.3%

say the accounting and finance teams work closely with their cybersecurity peers. In 2022, 22% experienced one breach, and 12.5% experienced multiple breaches. IBM estimates that 51% of businesses will increase security investments as a result of a breach, including incident response planning and testing, employee training, and threat detection and response technologies.

As set out by BDO, 2023 cyber threats cover a broad range of incidents, including:

- phishing and smishing;
- malware;
- ransomware;
- business email compromise;
- trusted insider threats (BDO cites one estimate that insiders represent 25% of data breaches);
- unintentional disclosure;
- storage reconnaissance for unprotected cloud storage;
- zero-day attacks exploiting previously unknown vulnerabilities;
- social engineering through fake personas and social media profiles; and
- data exfiltration.

The New Rules

Risk Management and Strategy

Domestic registrants must describe their processes, if any, for the assessment, identification and management of material risks from cybersecurity threats, and describe whether any risks from cybersecurity threats have materially affected or are reasonably likely to materially affect their business strategy, results of operations or financial condition (Regulation S-K, Item 106(b)). In providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure items:

- whether and how any such processes have been integrated into the registrant's overall risk management system or processes;
- whether the registrant engages assessors, consultants, auditors or other third parties in connection with any such processes; and
- whether the registrant has processes to oversee and identify such risks from cybersecurity threats associated with its use of any third-party service provider.

The SEC dropped the proposed requirement to disclose how a company plans for, defends against, or responds to, cyberattacks. The use of the term "processes" is intended to avoid disclosure of operational details that could be exploited by malign actors. The SEC also dropped a proposed list of risk types, and declined to require proposed disclosure around prevention and detection activities, continuity and recovery plans, and previous incidents.

Governance

Domestic registrants must describe in their annual reports on Form 10-K the board's oversight of risks from cybersecurity threats and management's role in assessing and managing material risks from cybersecurity threats (Regulation S-K, Item 106(c)). Foreign private issuers must provide the same disclosure in their annual reports on Form 20-F. In

providing such disclosure, a registrant should address, as applicable, the following non-exclusive list of disclosure items:

- whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant expertise of such persons or members in such detail as necessary to fully describe the nature of the expertise;
- the processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation and remediation of cybersecurity incidents; and
- whether such persons or committees report information about such risks to the board of directors or a board committee or subcommittee.

The SEC dropped the proposed requirement for disclosure of whether and how the board integrates cybersecurity into its business strategy, risk management and financial oversight. It also dropped a proposed requirement regarding cybersecurity expertise at the board level, in light of the expectation that the expertise will reside at the management level. That said, Item 407(h) of Regulation S-K, which requires reporting of material information regarding board structure and role in risk oversight generally, remains operative.

Material Cybersecurity Incidents

While the foregoing disclosure is to be provided on an annual basis, the SEC will now require current reporting of material cybersecurity incidents.

Scope of disclosure

Domestic registrants must disclose (i) any cybersecurity incident they experience that they determine to be material, and describe the material aspects of its nature, scope and timing and (ii) the material impact or reasonably likely material impact (Form 8-K, Item 1.05), including on its financial condition and results of operations. The inclusion of "financial condition and results of operations" is not exclusive; registrants should consider qualitative factors alongside quantitative factors in assessing the material impact of an incident. The release notes that harm to reputation, customer or vendor relationships, or competitiveness or 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 SEC was not persuaded to exempt disclosure regarding cybersecurity incidents affecting third-party systems used by registrants[3] or to provide a safe harbor for those disclosures. The rationale advanced by the SEC was that, given the centrality of the materiality determination, that determination should not be contingent upon where the relevant systems reside or who owns them. This then suggests that registrants should ensure that agreements with vendors

[3] At the of May, a number of government agencies, accounting firms, banks, colleges, pension funds and corporate businesses were alerted that they had been affected by a breach of the file-transfer software program MOVEit. The ransomware attack is believed to have been launched by a syndicate with ties to Russia, C10p, that exploited a zero-day vulnerability in the program. An IT firm that provides services to Medicare, Medicaid, loan servicers and other government programs announced yesterday that information on up to 10 million people may have been accessed as a result of the MOVEit hack.

and cloud infrastructure providers require timely notification of cybersecurity incidents that may be material to a registrant.

The SEC also was not persuaded to replace the Item 1.05 requirement with periodic reporting of material cybersecurity incidents on Forms 10-K or 10-Q.

What was omitted in the final rule

The SEC did not carry over from the proposal a requirement to disclose the status of remediation, whether the breach is ongoing or whether data were compromised. Disclosure of data theft, asset loss, intellectual property loss, reputational damage or business value loss would depend on a materiality analysis. The SEC also added an Instruction to provide that a "registrant 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."

Timing of disclosure

The Form 8-K must be filed within four business days after determining a cybersecurity incident was material. The SEC was not persuaded to modify the proposed timing requirement, given the narrowed focus of the disclosure on material impact. For example, the SEC declined to tie the disclosure to the point at which a registrant mitigates, contains, remediates or otherwise diminishes the harm caused by the incident.

As a corollary to the disclosure trigger, the new rules clarify that registrants must make a determination of materiality "without unreasonable delay" after discovery of an incident. A registrant could not, for example, delay disclosure by tying the disclosure to a determination by the board or a committee and intentionally delaying the determination. Similarly, modifying internal procedures to delay any internal reporting or assessment would constitute an unreasonable delay. The SEC notes that registrants should continue sharing information with other companies or government agencies about emerging threats. Such information sharing may not necessarily result in an Item 1.05 disclosure obligation.

The obligation to file the Item 1.05 disclosure is triggered once a company has developed information regarding an incident sufficient to make a materiality determination, and a decision to share information with other companies or government actors does not in itself necessarily constitute a determination of materiality. A registrant may alert similarly situated companies as well as government agencies immediately after discovering an incident and before determining materiality, so long as the registrant does not unreasonably delay its internal processes for determining materiality.

A registrant may delay filing if the US Attorney General determines immediate disclosure would pose a substantial risk to national security or public safety. An interagency communications process will be established for communications of any such determination to the SEC and affected registrants.

Failure to timely file the Form 8-K disclosure would not result in loss of Form S-3 eligibility. Item 1.05 disclosure will be eligible for the limited safe harbor from Section 10(b) and Rule 10b-5 liability. An Item 1.05 Form 8-K must be "filed," rather than "furnished."

To accommodate registrants subject to the Federal Communications Commission notification requirement (47 CFR § 64.2011) to the Federal Bureau of Investigation and US Secret Service for breaches of customary proprietary network information (CPNI), disclosure by these registrants can be delayed by up to seven business days following notification to the FBI and USSS, with written notification to the SEC.

In light of the four-day reporting deadline and the SEC's historical focus on disclosure controls and procedures, registrants should ensure they have the internal processes in place to run any potential disclosure through the SEC disclosure process, including review by the Disclosure Committee, if any. As part of the monitoring process, registrants should ensure that they are able to correlate, if needed, any current incident to past incidents.

Amending prior disclosure

Registrants must amend a prior Item 1.05 Form 8-K to disclose any information called for in Item 1.05(a) that was not determined or was unavailable at the time of the initial Form 8-K filing. If it is the case, in the initial filing, the registrant will have included a statement that the Item 1.05 disclosure is not complete as the information is not determined or is unavailable at the time of the required filing.

The SEC decided to withdraw a proposed requirement to update cybersecurity disclosure covered by Form 8-K disclosure, namely material changes, additions or updates thereof, in periodic reports. Updates are to be provided in a Form 8-K amendment.

The SEC also decided to withdraw a proposed requirement to provide disclosure when a series of previously undisclosed individually immaterial cybersecurity incidents become material in the aggregate. As the term "cybersecurity incident" is to be construed broadly to include "a series of related unauthorized occurrences," Item 1.05 may be triggered by what may appear as a series of related intrusions even if the material impact/reasonably likely material impact could be "parcelled among the multiple intrusion to render each by itself immaterial." This could occur, for example, if multiple actors exploit the same vulnerability, with the business then being materially impacted.

Foreign private issuers

Since foreign private issuers are not subject to Form 8-K reporting, they must furnish on Form 6-K information on material cybersecurity incidents that they disclose or otherwise publicize in a foreign jurisdiction, to any stock exchange, or to security holders (consistent with the overarching disclosure principle for Form 6-K reports).

Concluding Thoughts

Cyberthreats regrettably are a cost of doing business, and with the pace of advances in generative AI, cyberthreats are only likely to increase in scope and number.

But, despite the threat, to date, there have been no explicit ("line item") SEC cybersecurity disclosure obligations, resulting in a hodgepodge of disclosures that are not necessarily consistent, informative or timely. The SEC previously has noted that some registrants provide disclosure, while others do not. Disclosure that is provided varies considerably as to cause, scope, impact and materiality. Many include cyberthreats in risk factors, but at times those risks are bundled with other unrelated risks. That will now change, with the most

significant impact of the new rules likely to be that cybersecurity issues will no longer be viewed as being within the sole purview of the IT/security professionals in a company.

It bears repeating that the disclosure obligations under the 1933 and 1934 Acts, in general, and the 2011 and 2018 guidance, in particular, remain in effect, which means that registrants will still need to consider the impact of potential and actual cybersecurity incidents when preparing risk factors, MD&A, business descriptions, legal proceedings and financial statement disclosures, and need to stress test their disclosure controls and procedures as they relate to cybersecurity incidents. Regulation FD and insider trading considerations could also be relevant.

While not perfect, the SEC appears to have listened to industry and rolled back the more egregious elements of their initial proposal. As Commissioner Lizárraga noted, there are benefits to investors as well as the broader corporate landscape that will flow from the new rules. Disclosure will likely alert others in specific industries to threats they should be assessing as a pre-emptive measure.

Expect to see more on cybersecurity in light of the National Cybersecurity Strategy announced by the White House in March as well as the expected CISA rulemaking under the CIRCIA.

* * *

Mark S. Bergman
7Pillars Global Insights, LLC
Washington, D.C.
July 28, 2023