Cooley

SEC Reporting Implications for Publicly Traded Companies Impacted by CrowdStrike Defective Software Update

July 22, 2024

There are a number of US Securities and Exchange Commission (SEC) reporting implications arising from the server-related outages caused by CrowdStrike's defective software update on July 19, 2024, and their impacts on public companies, particularly in light of the SEC's new cybersecurity disclosure rules. While the situation on the ground – as well as answers to these questions – is still very much evolving, public companies impacted by the CrowdStrike update should consider doing the following:

- Ensure compliance with applicable policies and perform assessments to determine whether any impact from the CrowdStrike update is "material," and whether any reporting is necessary or advisable.
- Perform risk assessments and gap analyses to determine whether there are any shortcomings in systems and systems-related matters, including use of third parties and relevant oversight, monitoring, disaster recovery, and other practices.
- Update risk factors and other disclosures, including regarding systems downtime and/or reliance on third parties to operate critical business systems.
- Determine if the CrowdStrike update has had or is expected to have a material impact on the company, then consider if it should be discussed in the management's discussion and analysis (MD&A) section of SEC filings, including as a known trend for future periods.
- Be mindful of Regulation FD when communicating with analysts and investors regarding the impact of the CrowdStrike update on the company.
- Evaluate whether the CrowdStrike update has implications for the company's internal controls and disclosure controls and procedures.

Form 8-K and implications of CrowdStrike update

An immediate question in the context of real-time reporting on current reports on Form 8-K is whether the CrowdStrike-related server outages and other impacts on information and information systems of public companies could constitute "cybersecurity incidents" for purposes of Item 1.05 of Form 8-K.

With most third-party software programs deployed on company systems, public companies around the globe generally authorize providers to push periodic software updates to the companies' internal systems. Indeed, the deployment of such updates and security patches is often critical for companies to maintain an appropriate cybersecurity posture. However, the recent CrowdStrike update caused global, widespread and, in some cases, systemic failures to computers and networks of CrowdStrike's customers running certain Microsoft operating systems.

While CrowdStrike has stated that its defective code was not due to malicious activity, it is important to note the breadth of the SEC's definition of a reportable "cybersecurity incident" for purposes of Item 1.05 of Form 8-K in the adopting release for the final rule: "[A]n 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."[1]

This definition is easier to apply to malicious cyber occurrences that cause operational impacts such as ransomware or distributed denial of service (DDoS) attacks that jeopardize the availability of information systems or information. But it is more difficult to apply to operational impacts arising from faulty coding or technology outages, which may be day-to-day events for thousands of companies.

In fact, a related issue was raised during the comment period for the SEC's proposed cyber rule, and the SEC provided its views in the adopting release, stating that "[o]ne commenter sought clarification of whether the definition encompasses accidental incidents, **such as chance technology outages**, that do not involve a malicious actor, while another commenter advocated broadening the definition to any incident materially disrupting operations, regardless of what precipitated it"[2] (emphasis added).

In addition, the SEC said in the adopting release that it was "retaining 'unauthorized' in the incident definition as proposed. **In general, we believe that an accidental occurrence is an unauthorized occurrence**. Therefore, we note that an accidental occurrence may be a cybersecurity incident under our definition, even if there is no confirmed malicious activity. For example, if a company's customer data are accidentally exposed, allowing unauthorized access to such data, the data breach would constitute a 'cybersecurity incident' that would necessitate a materiality analysis to determine whether disclosure under Item 1.05 of Form 8-K is required"[3] (emphasis added).

While allowing for accidental occurrences to potentially constitute cybersecurity incidents, the SEC's specific example relates to **unauthorized access to data** arising from an **accidental occurrence**, not a chance technology **outage**. This example is relatively noncontroversial, as many data breach lawyers have long considered inadvertent data disclosures to be data breaches where the data ends up in the hands of an unauthorized person. However, it does not expressly address whether the additional element of unauthorized access to data is required for an accidental occurrence to constitute an unauthorized occurrence.

In our view, categorically construing the CrowdStrike update (or similar events) as an unauthorized occurrence would expand the definition of "cybersecurity incident" to potentially capture common software outages and disruptions that are simply baked into the use of software. It is important to note that the CrowdStrike update was authorized by the thousands of organizations that agreed to (and want to) receive automatic software updates from software companies such as CrowdStrike. Requiring real-time reporting on Form 8-K for material impacts of coding errors or software outages that occur in the ordinary course of business would not seem to further the SEC's objective of reducing mispricing of securities in the market in connection with material cybersecurity incidents and could have the opposite effect as investors may overreact to a disclosed accidental outage.

In addition, capturing accidental outages from authorized activity in the definition of "cybersecurity incident" would likely result in a significant increase in the number of Item 1.05 8-K disclosures, which would potentially obfuscate the reporting of material cybersecurity incidents truly important to investors and further frustrate the objectives of the new rules. Furthermore, systems outages like those experienced by companies following the CrowdStrike update are only one of many examples of operational disturbances that companies may experience, and there are potentially equally or more significant operational issues that a company might face (e.g., impacts from weather; natural disasters; labor, supplier, manufacturer, customer or lender issues; geopolitical, regulatory or financial markets issues) that generally may not trigger a required Form 8-K.

Even so, the issue is unsettled, and it is important to understand that the SEC has taken a broad interpretation of the federal securities laws with respect to cybersecurity compliance and disclosure matters. Moreover, plaintiffs' firms may seek to pursue actions based on a more expansive interpretation of the rules. As discussed below, public companies should bear in mind that the Form 8-K cybersecurity incident reporting requirements are not the only potential reporting considerations in the wake of the CrowdStrike update. Therefore, if a public company experienced impacts from the CrowdStrike update, it should be undertaking a materiality assessment of those impacts to determine if any reporting outside the context of Item 1.05 of Form 8-K is necessary or advisable.

Other SEC reporting considerations and takeaways

The North Star for many of the SEC's disclosure and reporting obligations is materiality: where there is a substantial likelihood that a reasonable shareholder would consider information about an occurrence important in making an investment decision, or if information about the occurrence would have significantly altered the "total mix" of information made available. Regardless of whether the CrowdStrike update constitutes a "cybersecurity incident" under the SEC's cybersecurity rules, public companies should consider whether the impacts from the CrowdStrike update might be material, qualitatively and/or quantitatively. If so, they should analyze applicable reporting provisions, including giving consideration to potentially providing voluntary disclosure related to the impact of the CrowdStrike update on the company's operations via Item 8.01 of Form 8-K[4], in addition to considering updating risk factors to address systems downtime and/or reliance on third parties to operate critical business systems to specifically refer to the CrowdStrike update. If the CrowdStrike update has had or is expected to have material impacts on the company reflected in current and/or future periods, then disclosure should be included in the MD&A, including as a known trend. These considerations should be kept in mind not only for periodic reports but also for registration statements, securities offering materials and other disclosures.

Companies also should be mindful of **Regulation FD** when communicating with analysts and investors regarding the impact of the CrowdStrike update on their business. Confirming that there was or was not a material impact of an occurrence in one-off communications with analysts/investors could be deemed to be a selective disclosure of material nonpublic information in certain circumstances. As a result, unless a company is prepared to make a statement in a Regulation FD-compliant manner, the best practice would be to simply respond to such inquiries with a statement that the company is aware of its obligations under securities laws.

Finally, based on the issues surrounding the CrowdStrike update (and inevitably similar ones to come), companies should continue maturing their incident response and escalation processes to enable prompt, reasonable and defensible materiality analysis, in addition to refining their corresponding controls and procedures. The CrowdStrike update reinforces how critical it is for companies to develop and operationalize processes applicable to technology issues that may arise not just from malicious attacks, but also from human error and coding failures or other disruptions. Companies should ensure that they are complying with any applicable policies, procedures and plans, including any escalation or "reporting up" procedures.

Companies also should continue to evaluate their systems, policies and practices in response to the CrowdStrike update (and other events) to identify risks and any gaps, including with respect to internal controls and disclosure controls and procedures, and take responsive measures by creating and refining policies, procedures, practices, and plans to ensure that impacts to their organization that may arise from cybersecurity threats, system downtime or outages, and other IT issues are appropriately addressed.

Please contact your Cooley lawyer or one of the lawyers listed below as you and your team work through these evolving considerations.

Cooley special counsel Luci Altman also contributed to this alert.

Notes

1. Release No. 33-11216, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (July 26, 2023), page 76.
2. *Id.*, pages 72 – 73 (emphasis added).
3. *Id.*, page 78 (emphasis added).
4. On May 21, 2024, **SEC Corporation Finance Director Erik Gerding published a statement** with explanatory guidance regarding cybersecurity incidents under Item 1.05 of Form 8-K. Gerding explained that only material cybersecurity incidents should be disclosed under Item 1.05 of Form 8-K. If a company

chooses to voluntarily disclose cybersecurity incidents that are not material or for which materiality has not yet been determined, they are encouraged to make such disclosures under Item 8.01 of Form 8-K.

Key Contacts

David Navetta Colorado	dnavetta@cooley.com +1 720 566 4153
Michael Egan Washington, DC	megan@cooley.com +1 202 776 2249
Sarah Sellers New York	ssellers@cooley.com +1 212 479 6370
Brad Goldberg New York	bgoldberg@cooley.com +1 212 479 6780
Jon Avina Palo Alto	javina@cooley.com +1 650 843 5307
David Peinsipp San Francisco	dpeinsipp@cooley.com +1 305 724 0538
Beth Sasfai New York	bsasfai@cooley.com +1 212 479 6081
Jaime L. Chase Washington, DC	jchase@cooley.com +1 202 728 7096

Reid Hooper Washington, DC	rhooper@cooley.com +1 202 776 2097
Amanda Weiss New York	alweiss@cooley.com +1 212 479 6858
Christian Lee San Francisco	christian.lee@cooley.com +1 415 693 2143