Published on *The National Law Review* https://natlawreview.com

SEC Cybersecurity Disclosure Trends: 2025 Update on Corporate Reporting Practices

Article By:

Jena M. Valdetero

Wouter van Wengen

Go-To Guide:

- Since April 2024, 41 companies disclosed cybersecurity incidents via Form 8-K, with 26 filing under voluntary Item 8.01 and 15 under mandatory Item 1.05, which requires reporting if the incident had a material impact on the company.
- Following the SEC's May 2024 guidance clarifying that Item 1.05 is intended only for mandatory filings, companies appear to be increasingly filing voluntary non-material cybersecurity incidents under Form 8-K Item 8.01 rather than under Item 1.05.
- Recent cybersecurity incident disclosures contain more detailed information about affected systems and compromised data, particularly in Item 1.05 filings, than the more general disclosures filed right after the rule became effective.
- Some amended Form 8-K filings under both rules focus on operational recovery status and typically conclude no material impact occurred, even under Item 1.05 filings.

Six months after the SEC's Cybersecurity Incident Disclosure Rule (SEC Rule) came into force, an April 2024 GT Alert summarized disclosure trends. The GT Alert identified that the companies who filed a mandatory form 8-K disclosing a cybersecurity incident had erred on the side of caution, hedged on whether the materiality threshold had been met or outright stated that it had not, reported an incident early, and provided only high-level information about the incident.

The SEC's Division of Corporation Finance (Corp Fin) issued clarifying guidance on May 21, 2024, noting that companies were filing materiality disclosures under new Item 1.05 for incidents that did not rise to the level of a material adverse event. In other words, companies possibly afraid of being second-guessed were opting to report under Item 1.05 even when they determined that the cybersecurity incident did not have a material adverse event. The SEC's guidance clarified that new Item 1.05 was only appropriate for cybersecurity incidents that had a material effect on the company and suggested companies could avail themselves of voluntary disclosure under Item 8.01 instead.

As a potential result of the May guidance, companies are increasingly filing non-material cyber incident disclosures under Item 8.01 of Form 8-K, while material incidents continue to be reported under Item 1.05. Since April 2024, 41 companies have filed a form 8-K to disclose a new cybersecurity incident, but 26 did so under 8.01 and 15 did so under 1.05.[1] Additionally, companies are providing more detailed disclosures about affected systems and data, but amended filings often lack clarity on when additional information was discovered and primarily confirm the resumption of operations with no material impact.

SEC Rule Disclosure Requirements

As a recap, the SEC Rule requires the following:

1. **Disclosure Requirement**: Companies must disclose material incidents within four business days of determining their materiality by filing a Form 8-K under Item 1.05.

2. **Materiality Determination**: The assessment of materiality must happen without unreasonable delay after discovering the incident. A cybersecurity incident is material if it has a "substantial likelihood that a reasonable shareholder would consider it important" in making an investment decision or would have "significantly altered the 'total mix' of information made available." There is no bright-line test for assessing materiality. When assessing materiality, the SEC directed public companies to consider both quantitative and qualitative factors, including the immediate consequences and long-term implications for operations, customer relationships, financial performance, brand reputation, and the likelihood of litigation or regulatory action.

3. **Delay Exception**: The only reason to delay disclosure is a written request from the U.S. Attorney General to protect national security or public safety.

4. **Form 8-K Content**: The form must include:
   - discovery date and status (ongoing or not),
   - description of the incident's nature and scope,
   - information about stolen or altered data,

- potential impact on operations, including financial effects, and
- remediation efforts or plans.

5. **Amended Form 8-K Filing**: Once this information becomes known, the SEC's Final Rule requires companies to amend a prior Form 8-K to disclose any information called for that was unavailable at the time of the initial Form 8-K filing. Amendments must be filed within four business days after the company, without unreasonable delay, determines such information or within four business days after such information becomes available.

Emerging Cybersecurity Incident Disclosure Trends

Looking at the disclosures companies have made up until today, there are five emerging trends:

1. **Disclosures of non-material incidents are increasingly filed under Item 8.01**. The SEC's guidance was effective in providing a roadmap for public companies to disclose incidents deemed initially immaterial under Item 8.01. Since then, more companies have started using Item 8.01 to disclose non-material cybersecurity incidents in their 8-K filings.

2. **Uptick in companies reporting material impact**. Since April 2024, there has been an uptick in companies disclosing a material impact of their cyber incidents under Item 1.05. Six out of 15 companies specified the material impact on their financial condition or results of operations in their disclosures under Item 1.05, whereas prior to April 2024, there were none. However, there are still no cases where the company later (in the amended Form 8-K) confirms that there was in fact material impact. So far, the amended disclosures conclude that there is no material impact or that material impact is reasonably unlikely.

3. **More detail in the disclosures**. Companies are starting to include more details in their 8-K filings than the first half of 2024. For instance,

companies report about the affected systems, particularly the impacted data, such as whether it contains sensitive personal information. On the other hand, filings under Item 8.01 have been considerably shorter, generally providing a high-level overview of the incident, as they do not need to meet the content requirements for the material incident disclosure under Item 1.05.

4. **Amended disclosures do not include the date when additional information was identified**. While an amended Form 8-K must be filed within four business days after additional information becomes available, companies do not indicate the date when they became aware of additional information on the incident. Hence, it cannot be determined whether companies have met the timing requirement.

5. **Amended disclosures often focus on the resumption of operations and confirm no material impact has been identified**. Generally, companies use the amended Form 8-K under both Items 1.05 and 8.01 (i) to indicate that they have resumed their normal business activities and (ii) to confirm that the incident does not or is unlikely to have a material impact.

[1] This number excludes amended filings.

National Law Review, Volume XV, Number 38