

SEC CYBERSECURITY DISCLOSURE RULE.



The SEC doesn't mandate how a company secures its systems — **it mandates that investors find out, within four business days of a materiality call, when something material happens.**

- 4-BUSINESS-DAY DISCLOSURE
- MATERIALITY DETERMINATION
- BOARD GOVERNANCE DISCLOSURE
- RELATED-INCIDENT AGGREGATION

01 THE MECHANISM

Materiality Determination Starts the Clock

The four-business-day countdown begins not at discovery, but when the company determines an incident is material — **and that determination itself must happen without unreasonable delay**, closing the option to slow-walk the call.

Existing Securities-Law Materiality, Not a New Standard

The SEC reused the decades-old reasonable-investor materiality test from securities fraud law rather than writing a cyber-specific bar — **reputational and regulatory harm can make an incident material** even without a quantifiable dollar loss.

Governance Disclosure, Not Technical Controls

The annual Item 106 disclosure describes the board's oversight and management's process for handling cyber risk — **the SEC never mandates a specific security control**, only that investors can see how the risk is governed.

02 THE FLOW

The Disclosure-Ready Company

CONTAINED

1

A cybersecurity incident is discovered, and the materiality assessment process, pre-built and rehearsed, runs without unreasonable delay to reach a documented determination.

2

Once material, the four-business-day Form 8-K clock is met with a disclosure that **describes the incident's nature, scope, and impact** without handing attackers a technical roadmap.

3

Related incidents from the same threat actor are **evaluated in aggregate**, so a pattern of smaller intrusions doesn't quietly avoid the materiality threshold.

The Reactive Company

EXPOSED

1

A cybersecurity incident is discovered, but the materiality call drifts for weeks while legal, IT, and executives debate informally with no documented process.

2

By the time a Form 8-K is filed, **the company has already missed the four-business-day window** measured from its own belated materiality determination, inviting SEC scrutiny of the delay itself.

3

Each related incident is assessed alone, so a string of individually "immaterial" intrusions from one threat actor **never triggers the aggregate materiality analysis** the rule requires.

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Form 8-K Item 1.05 Incident Disclosure	Requires disclosing a material cybersecurity incident within four business days of determining materiality, describing its nature, scope, and material impact.
Regulation S-K Item 106 Annual Disclosure	Requires an annual description of the registrant's cybersecurity risk management process and the board's oversight of that risk in the Form 10-K.
Reasonable-Investor Materiality Standard	Applies the existing securities-law materiality test, not a new cyber-specific bar, including qualitative harms like reputational and regulatory risk.
Aggregation of Related Incidents	Requires evaluating a series of related, individually immaterial incidents together, so a pattern from the same threat actor can't avoid the materiality threshold by being split apart.

04 DETECTION APPROACHES COMPARED

APPROACH	SUFFICIENT ALONE?	WHAT IT MISSES
Disclose Only Individually 'Big' Incidents	No	Misses the required aggregation analysis for a series of smaller, related incidents from the same threat actor that together could be material.
Start the Clock at Discovery, Not Determination	No	Misreads the rule's actual trigger, which is the materiality determination itself, made without unreasonable delay after discovery.
Include Full Technical Exploit Detail in the 8-K	No	Can hand attackers a roadmap and complicate an active response, without being required by the rule.
Ad Hoc, Undocumented Materiality Calls	No	Leaves no record showing the determination was made without unreasonable delay, inviting scrutiny of the disclosure timeline itself.
Pre-Built Materiality Process + Aggregation Review + Governance Disclosure + Documented Timeline	Yes	Meets the disclosure deadline defensibly, captures aggregated risk, and gives investors the governance picture the rule asks for.

SEC CYBERSECURITY DISCLOSURE RULE.

DETERMINE · DISCLOSE · GOVERN

05

PROGRAM OPERATIONS

This is a disclosure regime, not a security-controls mandate. The SEC never tells a company how to secure its systems — it requires timely, honest disclosure of material incidents and governance practices to investors.

The clock starts at the materiality determination, not discovery. That determination itself must happen without unreasonable delay, so slow-walking the decision doesn't buy extra time.

The SolarWinds action reshaped industry anxiety around this rule, even though it predated it — fraud charges against the company and its CISO became the reference point for personal liability, though a court later narrowed most claims against the CISO.

A national-security delay is the only built-in exception to the 4-day clock. Only the U.S. Attorney General can authorize one, and only for substantial national security or public safety risk.

06

CONTROL MAPPING

SEC FORM 8-K ITEM 1.05

The material-incident disclosure requirement, effective for most registrants beginning December 18, 2023.

REGULATION S-K ITEM 106

The annual cybersecurity governance disclosure requirement, covering risk management process and board oversight in the Form 10-K.

BASIC INC. V. LEVINSON MATERIALITY STANDARD

The existing securities-fraud materiality test the SEC reused rather than writing a new cyber-specific standard.

SEC V. SOLARWINDS

A securities-fraud enforcement action predating this rule that shaped industry expectations around disclosure and personal executive liability.

07

WHAT THIS DOES NOT SOLVE

State & Sector Breach Notification Laws

SEC disclosure runs **alongside, not instead of**, separate state breach notification laws and sector rules like GLBA or HIPAA that may also apply.

Private Companies

The rule binds **SEC reporting companies** — privately held companies outside the public markets fall entirely outside its scope.

Technical Remediation

Meeting the disclosure deadline says nothing about whether the underlying **vulnerability has actually been fixed**.

Non-Material Incidents

Incidents a company reasonably determines are **not material** carry no Item 1.05 disclosure obligation at all, regardless of how alarming they may look internally.

08

MYTHS VS. REALITY

MYTH "Every cybersecurity incident must be disclosed within four business days."	REALITY Only incidents determined to be material trigger the four-day clock — the rule doesn't require disclosing every intrusion, only ones a reasonable investor would consider important.
MYTH "The four-day clock starts when the incident is discovered."	REALITY It starts when the company determines the incident is material, though that determination itself must happen without unreasonable delay after discovery.
MYTH "The SEC requires companies to disclose their specific security vulnerabilities and technical details."	REALITY Disclosure covers nature, scope, and material impact — the SEC has said companies need not disclose technical details that could impede remediation.
MYTH "This rule tells companies what security controls to implement."	REALITY It's a disclosure and governance-transparency rule — the SEC does not mandate any specific security control.
MYTH "Splitting a large incident into smaller reported events avoids the materiality threshold."	REALITY The rule requires aggregating related incidents from the same threat actor or root cause, specifically to close that loophole.

09

SPEAK THE PROGRAM — KEY TERMS

ITEM 1.05 (FORM 8-K)

The current-report item requiring disclosure of a **material cybersecurity incident within four business days** of the materiality determination.

ITEM 106 (REGULATION S-K)

The annual disclosure requirement covering a registrant's **cybersecurity risk management process and board oversight**.

MATERIALITY DETERMINATION

The company's own documented judgment, made **without unreasonable delay** after discovery, on whether an incident is material to a reasonable investor.

AGGREGATION

The requirement to evaluate a **series of related, individually immaterial incidents together** for combined materiality.

NATIONAL SECURITY DELAY

The sole built-in exception letting the **U.S. Attorney General** **authorize delayed disclosure** for substantial national security or public safety risk.

REASONABLE INVESTOR STANDARD

The existing securities-law test asking whether a fact would be **important to a reasonable investor's decision-making**, reused here rather than a new cyber-specific bar.