Global Digital Forensics · Guide edition 2026-11-03 · evestigate.com/insights/secs-2nd-push-on-cyber-security-focuses-on-risk-assessment/

SEC DISCLOSURE EVIDENCE

Technical Evidence for SEC Materiality Determinations, Form 8-K Disclosure and Board Oversight

Once a public company determines a cyber incident is material, Form 8-K Item 1.05 is due in four business days, and the rules require the determination itself to be made without unreasonable delay. Preserve the cloud and endpoint record now so the committee decides on facts. Call (800) 868-8189 at any hour.

Published September 21, 2015 · Updated October 30, 2026

Primary Reference for This Guide

Start with SEC cybersecurity disclosure rule, File No. S7-09-22.

By Joseph Caruso, Founder, CEO and CTO, Global Digital Forensics

The Four Business Day Clock After Determining an Incident Is Material

Public companies and registered investment entities operate under strict Securities and Exchange Commission cybersecurity disclosure rules that require filing a Form 8-K under Item 1.05 within four business days of determining that a cybersecurity incident is material, alongside annual Form 10-K disclosures detailing board risk oversight and management assessment processes. A well documented materiality determination rests on prompt technical facts about what systems were affected, whether financial reporting integrity was touched and what volume of sensitive data was actually accessed or exfiltrated.

Giving Disclosure Counsel and Audit Committees Hard Technical Facts

When a public company or regulated financial adviser detects an intrusion, Global Digital Forensics performs high speed forensic analysis and data reconciliation engagements directly for retained securities counsel, audit committees and corporate security leaders. In place of worst case scenarios, our examiners rapidly analyze cloud unified audit logs, database query histories, network egress telemetry and endpoint artifacts to bound the true operational and informational scope of the event. Our objective technical findings give disclosure committees the concrete evidentiary record needed to document their materiality analysis and answer post incident SEC or shareholder scrutiny.

© 2026 Global Digital Forensics, Inc. All rights reserved.

What the Rule Says and What Starts the Clock

The Commission adopted the rules on July 26, 2023, and its press release states that registrants must "disclose material cybersecurity incidents they experience" and describe annually their cybersecurity risk management, strategy and governance. The Form 8-K disclosure under Item 1.05 describes the material aspects of the incident's nature, scope and timing and its material impact or reasonably likely material impact, and it is due four business days after the registrant determines the incident is material. The clock starts at the determination rather than at detection, and the rules require that determination to be made without unreasonable delay after discovery, which keeps the decision moving.

Two further features matter for how the technical work is run. A registrant may delay filing if the United States Attorney General determines that disclosure would pose a substantial risk to national security or public safety and notifies the Commission in writing, which is a narrow path reserved for rare cases. And where information required by Item 1.05 is not determined or is unavailable at the time of filing, the registrant says so and files an amendment when the information becomes available. That amendment mechanism is why the examination should produce dated interim findings with stated confidence rather than a single report at the end. The annual disclosure, under Item 106 of Regulation S K, describes processes, management's role and board oversight, and our financial services page describes how assessment records support it.

Our role in this structure is factual. Materiality is a legal judgment counsel and the disclosure committee make with reference to the total mix of information available to a reasonable investor, and the record we supply informs it. What we supply is the record the judgment rests on: which systems and data were affected, whether financial reporting systems were touched, whether the attacker persists, what the operational impact is and how confident each statement is. Delivering those facts quickly, in writing, with their basis, is what lets the committee document a determination that was made without unreasonable delay on the evidence available, and update it honestly as the evidence grows.

What the Record Can Establish Toward Materiality

The technical record is read for scope. The examiner reads authentication logs for which accounts were used and from where, endpoint telemetry and domain records for which hosts were touched and whether privilege was escalated, and database query logs and application audit trails for whether systems that feed financial reporting were accessed and whether data was altered. Egress and staging evidence is examined for whether data left and roughly how much. Cloud tenant audit logs, including the Microsoft 365 Unified Audit Log and the Entra sign in logs whose retention Microsoft documents at its reference page, are where the examiner traces mailbox and file access in the environments where most disclosure relevant intrusions now begin. The results are findings, dated and sourced.

Whether those facts amount to harm is the committee's judgment, and the record informs it. Whether a given scope is material depends on the business, the data, the customers affected, the operational consequences and the market's likely reaction, and those are judgments counsel and management make with the facts in hand. We keep to that line: the examiner reports scope fully and plainly, and the characterization belongs to the committee. The report states what was touched and what was untouched, with the coverage of the logs behind each negative finding. Our guide on reconciling incident facts for notification decisions shows how the same discipline narrows a state law notice.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Negative findings carry particular weight in a disclosure context and are built with care. A finding that the financial reporting systems were untouched, or that egress during the dwell period matched normal traffic, can separate a precautionary filing from a determination that the incident is not material, and it draws its strength from the log coverage behind it. We state that coverage in the report so the committee knows what the finding can bear. Our Microsoft 365 forensics page and business email compromise analysis page describe how tenant evidence is examined, since executive mailbox compromise is among the most common fact patterns a disclosure committee faces.

Running the Engagement on a Disclosure Timeline

The engagement begins under the direction of securities counsel with a triage in hours. We identify the systems and accounts believed affected, capture volatile data and images before containment changes them, and export the cloud and identity logs whose retention clocks are shortest first, because for a tenant on a thirty day retention tier that detected the intrusion in week three, the earliest activity is days from rolling off. We establish a working timeline of the intrusion from the artifacts available and deliver a first written interim finding to counsel with the basis and confidence for each statement. That first document is what lets the disclosure committee begin its deliberation on facts rather than on the worst case the security team fears.

Scoping continues in parallel with the committee's work and produces further dated interim findings as the record matures. Each one is written so a later reader can see what was known on what date, which documents that the company's disclosures tracked what it knew as it learned it. If a Form 8-K is filed with information not yet determined, the examination focuses on the open items so the amendment can be filed as soon as the facts are in. NIST Special Publication 800-61 Revision 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management, frames incident handling within the Cybersecurity Framework, and we use its structure so the method can be described to the committee and, later, to the Commission.

The final report consolidates the interim findings into a single account with each finding tied to a named artifact, hash and tool version, inferences labeled and the reach of each source stated. Counsel uses it for the amendment if one is needed, for responses to any Commission inquiry, and for the Form 10-K description of how the company assessed the incident. Our ransomware and data breach analysis page describes scoping for the most common incident types. Running the engagement as a sequence of dated written findings rather than a single late report is what protects the company's disclosure record, because the record then shows a committee deciding carefully on evidence as it emerged.

The Disclosure Cadence That Keeps a Filing Record Consistent

Four habits keep a disclosure record strong. The first is deciding on interim facts. The rule expects a determination without unreasonable delay, and a committee that documents its reasoning on interim facts and updates it as the record grows is in a strong position. The second is consistency, so the Form 8-K, the customer notice and any response to the Commission tell the same account. The third is a Form 10-K governance disclosure drawn from the processes the company actually runs, so the description matches the program when an incident tests it. The fourth is internal reporting kept to sourced facts, so any document that later becomes discoverable matches the filing.

© 2026 Global Digital Forensics, Inc. All rights reserved.

The cadence that supports them is built across the year. The annual cycle carries the penetration test, the readiness verification that the logs needed to scope an incident exist and are retained, and the Form 10-K disclosure drafted from the actual program rather than from a template. The quarterly cycle carries the CISO's report to the audit committee on control status and incidents. At least annually, a tabletop with securities counsel, the CISO, the disclosure committee and the response partner walks an incident from detection through determination, filing and amendment, so the four business day clock has been rehearsed with the actual people. Our penetration testing page describes the assessment component.

When a disclosure is later challenged, by the Commission or by shareholders, the technical record is examined alongside the committee's minutes. Our examiners have testified in federal and state courts and our work has been accepted by courts, and every disclosure engagement is run so that the examiner can stand behind each interim finding as of its date. Our securities fraud case study describes how we obtained and rebuilt a decade of clearing firm transaction records in support of counsel in a complex financial matter, and our expert witness services page describes how a report moves to declaration and testimony. A company that can show it decided on dated facts, supplied by an examiner who stands behind them, has built its disclosure record on the strongest footing available.

Prepare Your Disclosure Evidence Workflow Before an Incident

Align your technical incident response plan with your legal disclosure obligations today. Our guide to reconciling enterprise data records after a breach shows how the same evidence narrows a notification decision. Call Global Digital Forensics 24/7 at (800) 868-8189 to brief your general counsel and CISO on rapid materiality scoping. The initial consultation is free.

What the Record Can Establish Toward Materiality

The guide keeps a firm line between the scope facts an examiner supplies and the materiality judgment counsel makes. This table lists the scope questions the technical record answers, the source behind each and the scope of each finding, so a disclosure committee can document a determination on dated facts. The third column keeps each finding at its true weight: the record speaks to scope, and the committee judges harm. The four business day clock starts at the determination of materiality rather than at detection.

Scope questions the record answers toward a materiality analysis, the source behind each and the scope of its finding.

Scope question	Source	Scope of the finding
Which accounts were used and from where	Authentication and sign in logs	The infrastructure behind a session; tying it to a person adds corroboration
Which hosts were touched	Endpoint telemetry and domain records	Hosts where telemetry was deployed and retained
Whether financial reporting systems were accessed	Database query logs and application audit trails	Systems where those logs were enabled

© 2026 Global Digital Forensics, Inc. All rights reserved.

Scope question	Source	Scope of the finding
Whether data left and roughly how much	Egress and staging evidence	Volume; the examiner looks for content in packet capture or staged archives
Mailbox and file access	Unified Audit Log and Entra sign in logs	Seven, thirty or 180 days by license per Microsoft
Whether the incident is material	A legal and business judgment	Counsel and management judge harm on the examiner's facts

The securities fraud case study describes correcting and rebuilding a decade of transaction records so counsel could form their arguments, the dated and sourced record a disclosure committee needs to document a determination.

How to Begin and What Happens on the First Call

Have the discovery date and what was observed, the systems and accounts believed affected, your cloud tenant licensing tier and log retention settings, the names of securities counsel and the disclosure committee members, your incident response plan, and any steps already taken toward containment. The examiner asks whether financial reporting systems may have been touched, whether the attacker may persist, what logging exists for egress and authentication, whether anything has been rebuilt, and how often the committee needs written interim findings. Counsel then receives a written preservation and scoping plan, a schedule of interim findings aligned to the determination and filing clocks, and a written proposal. The initial consultation is free, and the hotline at (800) 868-8189 answers at any hour.

Technical References and Further Reading

Earlier reporting on this subject: SEC OCIE 2015 Cybersecurity Examination Initiative risk alert.

Authorities cited in this guide: SEC press release 2023 139, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure. Establishes the Item 1.05 four business day disclosure after a materiality determination and the annual governance disclosure, release dated July 26, 2023. Microsoft Entra reports data retention. Establishes the seven day and thirty day retention of Entra sign in and audit logs by license tier, current Microsoft Learn reference page. NIST SP 800-61 Revision 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management. Establishes the incident handling structure we describe to disclosure committees and regulators, Revision 3 final publication.

© 2026 Global Digital Forensics, Inc. All rights reserved.

FREQUENTLY ASKED

Questions Counsel and Security Leaders Ask About SEC Disclosure Evidence

When is a Form 8-K cybersecurity disclosure due?

Item 1.05 of Form 8-K is due four business days after the registrant determines that a cybersecurity incident is material, a clock that starts at the determination rather than at discovery. The rules require the materiality determination to be made without unreasonable delay after discovery. A limited delay is available only if the Attorney General determines disclosure would pose a substantial risk to national security or public safety and notifies the Commission in writing. Information not yet determined is disclosed by amendment when available.

Who decides whether a cyber incident is material?

Counsel, management and the disclosure committee make that judgment with reference to what a reasonable investor would consider important, in light of the total mix of information. The forensic examination informs it. What we supply is the factual record the judgment rests on: which systems and data were affected, whether financial reporting systems were touched, whether the attacker persists and what the operational impact is, each with its basis and confidence, delivered in dated written findings as the record matures.

How quickly can forensic findings support a materiality determination?

Preservation and a first written interim finding happen in hours to days, depending on how fast the company can produce images and log exports and how short the cloud retention clocks are. Full scoping takes longer and depends on the number of systems involved, the quality of logging and whether data was staged and exfiltrated. We deliver dated interim findings throughout so the committee can begin its deliberation immediately and document how its understanding evolved rather than waiting for a final report.

What should a public company preserve when it suspects a material cyber incident?

Memory and images of affected hosts before any rebuild, domain controller and endpoint logs, firewall, proxy and VPN logs, the Microsoft 365 Unified Audit Log and Entra sign in and audit logs before their retention windows close, database and application audit trails for systems that feed financial reporting, email and messaging for the accounts involved, and a dated log of every response decision. Preserving those sources is what lets the examination produce the negative findings a careful determination often depends on.

What does an SEC disclosure forensic engagement cost?

Cost follows the number of systems and tenants in scope, how well the environment was logged, whether exfiltration analysis is needed, the frequency of interim written findings the committee requires, and whether the matter is likely to proceed to a Commission inquiry or shareholder litigation requiring a declaration or testimony. A contained executive mailbox compromise is a different engagement from a domain wide intrusion touching financial systems. The initial consultation is free and the proposal fixes the scope before work begins.

© 2026 Global Digital Forensics, Inc. All rights reserved.

Web Addresses for the Sources Cited

1. SEC cybersecurity disclosure rule, File No. S7-09-22: https://www.sec.gov/rules-regulations/2023/07/s7-09-22
2. press release: https://www.sec.gov/newsroom/press-releases/2023-139
3. its reference page: https://learn.microsoft.com/en-us/entra/identity/monitoring-health/reference-reports-data-retention
4. Incident Response Recommendations and Considerations for Cybersecurity Risk Management: https://csrc.nist.gov/pubs/sp/800/61/r3/final
5. SEC OCIE 2015 Cybersecurity Examination Initiative risk alert: https://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf

Reviewed by Joseph Caruso, Founder, CEO and CTO, CISSP. Last reviewed October 31, 2026.

Start With a Free Consultation

The initial consultation is free, and requests are handled in confidence. On the first call a senior member of our team listens to the question you need answered, identifies the records and systems involved, and recommends the next step.

Call (800) 868-8189, answered 24/7, request a consultation at evestigate.com/contact, or email info@evestigate.com.

© 2026 Global Digital Forensics, Inc. All rights reserved.