

Incident Analysis

This category asks whether you can determine what actually happened during an incident — root cause, scope, and exactly which data was touched — while preserving the evidence that proves it.

Why it matters

- Whether the district must notify families, staff or the state depends on which records were actually accessed. Without logs and a careful scope, leaders are left choosing between notifying broadly, which alarms the community and adds cost, and staying silent without proof, which carries legal risk.
- Wiping a laptop or deleting a compromised mailbox feels like progress but can destroy the evidence that forensic investigators, breach counsel and the insurance carrier need. Preserving evidence first keeps both the insurance claim and the notification decision on solid ground.
- Finding the real root cause, such as a staff account without multi-factor authentication (MFA) or a mail-forwarding rule nobody noticed, is what keeps the same attacker from returning through the same door. Stopping at "we fixed it" can mean living through the same incident again a few weeks later.

The stakes are concrete: state breach-notification laws turn on whose records were accessed, so bad scoping means either notifying thousands of families unnecessarily or facing legal exposure for staying silent. Your carrier's forensics team and breach counsel also depend on intact logs and a clean timeline; reimaging a machine too early can undermine both the investigation and the insurance claim.

What good looks like at each level

Level	What you would see	Artifacts that show it
1 · Initial	<p>When something goes wrong, the goal is to get things working again, and no one records what happened or why. Machines are wiped and passwords reset before anyone asks how the attacker got in or what data was touched.</p> <p>Moving up: Stop treating analysis as optional cleanup: adopt a cross-functional review for every incident (IT plus the data owner and an administrator) and start writing down a repeatable examination process instead of ad hoc recovery.</p>	<ul style="list-style-type: none"> • No incident record beyond a closed help desk ticket marked "fixed" • No one can say whether audit logging is on, or how long logs are kept, for Google Workspace or Microsoft 365, the firewall or the SIS • No rule against reimaging devices or deleting accounts before evidence is preserved
2 · Repeatable	<p>Incidents are reviewed by more than one person: the technology team, the owner of the affected data and an administrator. A repeatable way to examine incidents is being written down, and the team has started checking which logs exist before they are needed.</p> <p>Moving up: Analyze and categorize every incident consistently with the response plan — including an explicit check of federal and state notification triggers — evaluate findings systematically, and bring in third-party analysis (MS-ISAC, carrier forensics) for significant events.</p>	<ul style="list-style-type: none"> • Incident review notes showing who took part, such as the technology director, the SIS coordinator and an assistant superintendent • Draft analysis checklist and incident timeline template • List of log sources with their current retention periods
3 · Defined	<p>Every incident is categorized with the plan's severity scale and gets a written record with a timeline, root cause and scope. Each record documents whether student or staff records were involved and what that means under the Family Educational Rights and Privacy Act (FERPA) and state law, and significant incidents get outside analysis.</p> <p>Moving up: Push past 'what happened' to why: root-cause incidents down to the specific control or subprocess that failed, and use accumulated analysis to build risk inventories that set response levels in advance.</p>	<ul style="list-style-type: none"> • Incident records with timeline, root cause, affected accounts and systems, and a written data-scope determination • Audit logging enabled on email, the SIS and network security devices, with at least 90 days of retention • Forensic report from the carrier's panel firm, or analysis from MS-ISAC or a state partner, for a significant incident

Level	What you would see	Artifacts that show it
4 · Managed	<p>Analysis goes past what happened to the specific control or step that failed, such as a missing Conditional Access policy or a vendor account no one reviewed, and those findings change configurations and procedures. A risk inventory built from past incidents sets the response level for recurring incident types in advance.</p> <p>Moving up: Analyze across incidents, not just within them: trend the year's events to find systemic shortfalls and performance gaps, and give knowledgeable staff standing time to assess the full landscape for improvement opportunities.</p>	<ul style="list-style-type: none"> • Root-cause write-ups that name the failed control and the configuration or procedure change made • Risk inventory mapping recurring incident types, such as phished staff accounts or lost devices, to a predetermined severity and response • Twice-yearly summary to the superintendent of analysis findings and the status of corrective actions
5 · Optimized	<p>The district looks across a full year of incidents, near misses and exercises for patterns, such as repeated account compromises in one department or slow detection over school breaks. A standing group of technology staff meets regularly to review the whole security picture and propose improvements.</p>	<ul style="list-style-type: none"> • Annual incident trend review listing the gaps found and the improvement projects they produced • Quarterly meeting notes from the technology staff security review • Measures such as time from first report to completed scope determination, tracked from year to year

Quick wins

Quick win and how	Cost	Effort	Usual owner
<p>Verify Microsoft 365 unified audit logging or Google Workspace audit logs are enabled, and note retention windows</p> <p>In the Microsoft Purview portal, open Audit and confirm activity recording is on; in the Google Admin console, open Reporting, then Audit and investigation, and confirm login, Gmail, Drive and admin events are appearing. Write down how far back each log goes, then do the same for the firewall, content filter and SIS.</p>	Free	Hours	Network and systems administrator
<p>Create a blank incident-timeline template today</p> <p>Build a shared spreadsheet with columns for date and time, who observed or did what, the system affected, and where the supporting evidence is stored, and keep a printed copy with the plan. Use it in the next tabletop so the team has filled it in once before they need it.</p>	Free	Hours	Technology director
<p>Add a written 'preserve before you fix — no reimaging until cleared' rule to the IR plan</p> <p>Add a short section to the incident response plan stating that affected devices are isolated rather than wiped and compromised accounts are suspended rather than deleted until the carrier's forensic firm or legal counsel authorizes release. Brief the help desk and field technicians, since they are the ones most likely to reimage a machine out of habit.</p>	Free	Hours	Technology director
<p>Draft a ten-question scoping checklist: which accounts, which systems, which data</p> <p>Include questions such as which accounts signed in and from where, which mailboxes and shared drives were opened, whether SIS reports or exports were run, and whether files held special education, health or Social Security number data. Review the draft with the SIS coordinator, HR and the technology director so it points to where records actually live.</p>	Free	Hours	Data privacy officer
<p>Do a dry run: pull the audit logs from your last security event and file them with the ticket</p> <p>Pick a recent phished account or suspicious sign-in, export the sign-in and mailbox activity for those days from the Google or Microsoft admin console, and attach the export to the original help desk ticket. Write down anything you could not find; those gaps become your logging to-do list.</p>	Free	Hours	Network and systems administrator

Free means staff time, existing licenses or free government services. Effort: hours, days or weeks.

Common pitfalls

- Reimaging first and asking questions later. Wiping a laptop or deleting a mailbox can destroy the only proof of what the attacker reached; suspend, isolate and preserve until the carrier's forensic firm or counsel clears release.
- Discovering log gaps in the middle of an incident. Default retention in cloud consoles, firewalls and the SIS may not reach back to the start of an intrusion found weeks later, so check settings now and extend retention or export logs where needed.
- Stopping at the symptom. "A teacher clicked a phishing link" is not a root cause; ask why the click turned into access, such as a missing multi-factor authentication (MFA) requirement or an overly broad admin role, and fix that.
- Scoping without the people who know where data lives. The technology team may not know which shared drives hold special education records or which staff run SIS exports to spreadsheets; bring in the SIS coordinator, special education director, HR and the data privacy officer before deciding what was exposed.
- Writing incident notes without considering who may read them. Investigation records can be requested later through litigation or public records requests, so ask counsel early how to organize investigation work and keep notes factual rather than speculative.

Evidence that proves it

- Screenshots of audit-log settings and retention periods (Google Workspace or Microsoft 365, firewall, content filter)
- Incident timeline document from a past incident or exercise
- Completed after-action report identifying root cause
- Written evidence-preservation rule (no reimaging until cleared) in the IR plan
- Exported log samples or investigation-tool queries attached to an incident ticket
- Scope worksheet counting affected accounts, systems, and records
- MS-ISAC or forensic vendor analysis report

Who usually owns it

Technology director

Leads the investigation, keeps the incident timeline and evidence, coordinates outside forensic help, and writes the after-action report with root cause and corrective actions.

Network and systems administrator

Keeps audit logging and retention configured before incidents, pulls and preserves logs during one, and isolates rather than wipes affected systems.

Data privacy officer

Determines which student and staff records were involved, working with the SIS coordinator, HR and special education to confirm where data lives.

Legal counsel

Advises on evidence handling and on whether the findings trigger obligations under FERPA, state breach-notification law or vendor contracts.

Insurance relevance · Medium

Applications usually reach this area through questions about log collection, retention and alert handling rather than incident analysis itself. After a claim, the carrier's forensic firm depends on the logs and evidence the district kept, so gaps or early cleanup can slow the investigation and complicate the claim.

- Do you centrally collect authentication, endpoint, network and cloud logs, and how long do you keep them?
- Have you had a cyber incident in recent years, and what was the root cause and the corrective action?
- Will you use the carrier's approved forensic firm and preserve affected systems until it has reviewed them?
- Who reviews security alerts and decides when an event becomes an incident?

Tip: Check the actual retention setting in each console before you state a number on the application, because the carrier's forensic firm will learn quickly whether the logs go back as far as the answer says.

Funding and free help

CISA K-12 cybersecurity resources and toolkit

Always available

Free federal guidance for K-12: the K-12 cybersecurity report and toolkit, plus access to regional CISA advisors and no-cost services. A resource, not funding.

Programs, eligibility and deadlines change; confirm on the official page before applying.

Learn more

- Best Practices for Event Logging and Threat Detection (CISA) <https://www.cisa.gov/resources-tools/resources/best-practices-event-logging-and-threat-detection>
- SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile (NIST) <https://csrc.nist.gov/pubs/sp/800/61/r3/final>
- Protecting Student Privacy (U.S. Department of Education) <https://studentprivacy.ed.gov/>
- Multi-State Information Sharing and Analysis Center (MS-ISAC) (CIS) <https://www.cisecurity.org/ms-isac>
- CIS Critical Security Controls Implementation Group 1 (CIS) <https://www.cisecurity.org/controls/implementation-groups/ig1>