

Telling People and Handing It Over: Incident Reporting and eDiscovery

Mon, Sep 7, 10:00 AM EDT · <https://scottslab.io/posts/incident-reporting-and-ediscovery>



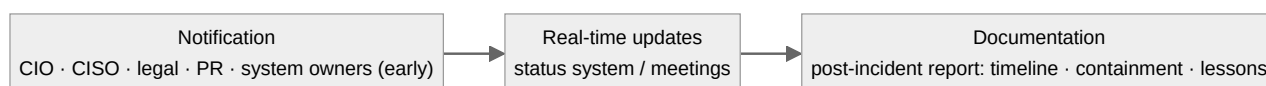
TL;DR

Incident reporting has three parts: notification (alert CIO, CISO, legal, PR, system owners early), real-time updates, and a formal post-incident report. Some incidents require external notice: CISA, or ISACs for industry sharing, and eventually mandatory 72-hour reporting for covered critical-infrastructure entities under CIRCIA, once its still-pending final rule takes effect. eDiscovery runs the fuller EDRM: identification, preservation, collection, processing, review, analysis, production, presentation. The two rules that decide whether you get sanctioned are FRCP 26(b)(1) (discovery has to be proportional, not unlimited) and FRCP 37(e) (losing electronic evidence you should have preserved can cost you the case, but only the worse tier requires proving you meant to).

Once you've investigated, two processes govern how the information leaves your hands: one for incidents, one for lawsuits.

Incident reporting

Incident reporting has three components, and skipping any one of them is how a technical win becomes an organizational mess. Notification is alerting the key stakeholders early: the CIO, CISO, legal, PR, and the system owners. They can't manage the fallout if they hear about it late. Real-time updates keep everyone current as things develop, through an automated status system or standing meetings, so nobody's operating on stale information mid-incident. And documentation is the formal post-incident report after the dust settles: the timeline, what contained it, and the lessons learned. That last part is the one people cut when they're tired, and it's the one that makes the next incident less painful.



Incident reporting

Some incidents don't stay internal. External notification may be required to CISA, or to ISACs (Information Sharing and Analysis Centers) for sharing threat information across an industry. A bigger obligation is on the way but isn't law yet: the **Cyber Incident Reporting for Critical Infrastructure Act (CIRCA)**, signed in 2022, would require covered critical-infrastructure entities to report substantial cyber incidents to CISA within **72 hours** and ransomware payments within **24 hours**. CISA published a proposed rule in April 2024, and as of this writing the final rule still hasn't taken effect. Reporting on it in mid-2026 still describes it as expected "this fall." Knowing your obligations here in advance matters regardless of exactly when the rule lands, because the middle of a breach is a bad time to discover you were legally required to tell someone six hours ago.

eDiscovery: the fuller model

eDiscovery is the parallel process once litigation is involved, and the three-stage version most people learn (preserve, collect, produce) is a simplification of the actual **Electronic Discovery Reference Model (EDRM)**: identification, preservation, collection, processing, review, analysis, production, presentation. The extra stages matter in practice. Processing is where raw native files get converted and their text and metadata extracted so a review platform can actually search them. Review and analysis are where attorneys separate the relevant from the irrelevant and the privileged from the discoverable. That's a step that's easy to conflate with production but is legally distinct from it, since privilege gets asserted here, before anything crosses to the other side.



eDiscovery: the fuller model

When the duty to preserve actually starts

Preservation isn't triggered by a lawsuit being filed. It's triggered by litigation being **reasonably anticipated**, which can be well before anyone files anything. This comes from *Zubulake v. UBS Warburg* (S.D.N.Y. 2003–2005), the case most modern e-discovery practice traces back to: Judge Shira Scheindlin held that once litigation is reasonably anticipated, a party has to issue a written litigation hold, and failing to do so can itself be found grossly negligent. That's the legal basis for the rule you'll hear repeated everywhere: the routine 30-day log rotation that's normally good hygiene becomes destruction of evidence the moment a hold should have gone out. That's true whether or not one actually did.

Two Federal Rules of Civil Procedure decide what happens if you get this wrong, and they're worth knowing by number, not just by vibe. **FRCP 26(b)(1)** sets discovery's actual scope: material has to be relevant *and* "proportional to the needs of the case," weighing the amount in controversy, the parties' resources, and whether the burden of producing it outweighs its likely benefit. Discovery isn't a blank check to demand everything. **FRCP 37(e)** governs what happens when electronically stored information that should have been preserved is lost because a party failed to take reasonable steps to preserve it. It has two tiers, and the difference between them is the whole ballgame: if the court just finds *prejudice* to the other side, it can order measures no greater than necessary to fix that prejudice. But if the court finds the party **acted with intent to deprive** the other side of the evidence, it can go much further: presuming the lost information was unfavorable, instructing the jury to presume the same, or dismissing the case outright. Losing evidence through negligence is a manageable problem; losing it in a way that looks intentional is how a case gets decided against you before a jury ever sees the merits.

The reassuring part, held honestly

Most litigation holds never reach production. Cases settle, or get dropped, long before anyone reviews the collected material. But you can't bet on that up front. The preservation obligation attaches the instant a hold is reasonably anticipated, so the log purge you let run "because it probably won't matter" is exactly the one that turns a defensible position into a spoliation problem under 37(e). Preserve first, and let the lawyers decide later what actually gets handed over.