THE OVERLOOKED PITFALLS

eDiscovery failures often occur when cybersecurity incidents and litigation overlap, creating risks around evidence preservation, cloud log retention, privilege, metadata, and cross-border data. Learn how legal, security, and forensic teams can coordinate during the critical first 72 hours to build a defensible response and protect critical evidence.

EDISCOVERY FAILURES AT THE INTERSECTION OF CYBERSECURITY INCIDENTS AND LITIGATION

The eDiscovery community knows the fundamentals. Preserve early. Collect defensibly. Document everything. But when a cybersecurity incident triggers litigation, the familiar playbook breaks down in ways that even experienced practitioners fail to anticipate. The overlap between incident response and discovery obligation creates a set of recurring, costly, and largely avoidable failures.

This paper identifies six of the most consequential breakdowns that show up in sanctions motions, adverse inference rulings, privilege disputes, and settlement negotiations across federal and state dockets every year. These happen to practitioners who know better because knowledge of the pitfall and preparation for it are two different things. For each one, IST's forensic and eDiscovery team has a direct answer.

Who this is for: Practitioners, corporate counsel, and legal operations professionals who already understand eDiscovery and want a focused look at where the process fails specifically when a cybersecurity incident is in the chain of events and how IST resolves each failure.

THE SIX PITFALLS

1 THE PRESERVATION OBLIGATION ATTACHES BEFORE YOU THINK IT DOES

What it looks like: The security team discovers an intrusion. Legal is notified 48 hours later, after initial triage. By then, affected systems have been reimaged and logs rotated.

Why it keeps happening: Incident response and legal hold are treated as sequential, not simultaneous. Security moves first; legal cleans up after. In most organizations, no protocol exists to trigger a hold at the moment of breach discovery.

Case impact: Evidence destroyed before the hold attached is spoliation regardless of intent. Courts evaluate the preservation obligation from the moment litigation was reasonably anticipated, not from when counsel was looped in. In a breach involving personal data, regulatory exposure, or a known plaintiff class, that moment is often the same hour the breach is confirmed.

IST Solution: IST's forensic team engages from the moment of incident discovery, not after remediation has begun. Our Strategic Pre-Analysis process establishes the legal hold framework in parallel with the security team's triage, ensuring preservation decisions are made before evidence is at risk. IST's project managers are available 24/7/365 to mobilize immediately when a breach is confirmed.

2 CLOUD AND SAAS LOGS DISAPPEAR ON A SCHEDULE NOBODY CHECKED

What it looks like: The forensic investigation completes. Counsel requests VPN access logs, identity provider records, and collaboration platform activity. The relevant window expired 47 days ago. Default retention was 30 days.

Why it keeps happening: Cloud log retention periods are set by platform administrators, not legal teams. Most organizations have never audited them. The 30–90 day defaults on common enterprise platforms, like Microsoft 365, Okta, Salesforce, Slack, are widely unknown outside the IT department.

Case impact: The most probative evidence of who accessed what, when, and from where is gone before anyone thought to look for it. In a data exfiltration matter, this is the case. Plaintiffs will draw the worst available inference from the gap.

IST Solution: IST conducts cloud and SaaS forensic collections across the full enterprise environment, including Microsoft 365, Google Workspace, Slack, Salesforce, iCloud, and identity provider platforms. Our pre-engagement data mapping identifies default retention windows before they close, and our team works with IT to extend log preservation immediately upon engagement. We collect what others miss before the window does.

3 THE FORENSIC INVESTIGATION REPORT IS NOT AS PROTECTED AS YOU THINK

What it looks like: Outside counsel engages a forensic vendor. The vendor delivers a report. Months later, opposing counsel moves to compel it, arguing the primary purpose was business remediation, not legal advice.

Why it keeps happening: Privilege protection for breach investigation reports is contingent on structure, not engagement. Reports delivered to business units, used to satisfy regulatory inquiries, or drafted before outside counsel formally retains the vendor are all vulnerable. The engagement letter is often an afterthought.

Case impact: Compelled production of the forensic report hands opposing counsel the full roadmap of the breach: what happened, what was accessed, what the organization knew and when. It also opens the door to subject matter waiver over related communications.

IST Solution: IST is engaged at the direction of outside counsel, with privilege structuring built into every forensic engagement from the outset. Our retention agreements are designed to support attorney-client privilege and work product protection. Reporting flows to counsel, not to business units. When the privilege of our investigation is challenged, IST's certified forensic examiners are available to provide expert witness testimony on the methodology and structure of the engagement.

REMEDIATION OVERWRITES THE METADATA THAT PROVES SCOPE 4

What it looks like: Ransomware encrypts a server environment. IT restores from backup. The encrypted file timestamps, which would have established exactly which files were affected and when, are overwritten in the restoration process.

Why it keeps happening: Restoration protocols are designed for operational continuity, not evidence preservation. IT teams are measured on recovery time, not forensic integrity. The two objectives are in direct tension, and absent a specific protocol requiring forensic imaging before restoration, continuity wins.

Case impact: Without the original encryption timestamps, the organization cannot demonstrate the precise scope of affected data. Regulatory notifications become estimates. Opposing counsel argues the worst case. The burden of proof, which should fall on plaintiffs, effectively reverses.

IST Solution: IST's forensic team creates complete forensic images of affected systems before any remediation activity begins, preserving encryption timestamps, file system metadata, and all artifacts of the attack. Using Cellebrite, Magnet Axiom, and write-blocking hardware, we capture the full evidentiary record in an unmodified state with cryptographic hash verification to confirm integrity. Remediation can proceed. The evidence stays intact.

5 THE NOTIFICATION LETTER BECOMES THE PLAINTIFF'S DISCOVERY ROADMAP

What it looks like: A breach notification is sent to affected individuals describing the categories of data potentially accessed. The class action complaint, filed six days later, mirrors the notification almost exactly and demands production of everything the notification described.

Why it keeps happening: Notification content is drafted under regulatory deadline pressure, often before the forensic investigation is complete. It describes potential exposure conservatively but broadly. Nobody has assessed what privilege consequences will flow from those descriptions in discovery.

Case impact: Plaintiffs treat the notification as a party admission. Every category of data described as "potentially affected" becomes a discovery target. Counsel who failed to anticipate this will find themselves producing far more than the forensic record actually supports or spending significant resources fighting requests the notification letter invited.

IST Solution: IST's forensic investigation defines the precise scope of affected data before notifications are finalized giving counsel the factual foundation to draft notifications that are accurate, specific, and strategically defensible rather than conservatively overbroad. Our project managers work alongside legal teams during the notification drafting process to ensure the forensic record and the notification are aligned. What you say in the notification shapes the discovery you'll face. IST helps you say it right.

6 CROSS-BORDER DATA IS COLLECTED FIRST, RESTRICTED LATER

What it looks like: A U.S. court orders production of data from an EU subsidiary. The collection proceeds. Six weeks later, opposing counsel in the parallel EU regulatory proceeding argues that the U.S. production constituted an unauthorized transfer of personal data under GDPR Article 44.

Why it keeps happening: U.S.-based counsel focuses on U.S. discovery obligations. Data transfer restrictions under GDPR, Swiss DPA, or other frameworks are either unknown or assumed to be someone else's problem. The collection happens before the legal analysis does.

Case impact: The organization now faces potential regulatory enforcement in the EU for the transfer, a challenge to the admissibility of the collected data in the U.S. proceeding, and the cost of negotiating a retroactive solution. None of this was necessary. Advance analysis of transfer mechanisms (Standard Contractual Clauses, derogations for legal proceedings, Hague Evidence Convention procedures) takes days. The cleanup takes months.

IST Solution: IST's Global Digital Forensics team supports national and international collections with proven adherence to international data standards, including GDPR, Swiss DPA, and applicable cross-border transfer frameworks. Our US-based data hosting is SOC 2 Type II, ISO 27001, HITRUST, and PCI compliant. We conduct the transfer mechanism analysis before collection begins so the evidence gathered is admissible on both sides of the proceeding.

WHAT THESE FAILURES HAVE IN COMMON

Each of the six pitfalls above shares a structural cause: the decision was made by the wrong team, at the wrong time, without the legal and forensic disciplines in the room together. Incident response is a technical function. Discovery is a legal one and the overlap between the 72-hour window where evidence is created, preserved, or lost forever is almost never governed by a protocol that brings both disciplines to the same table simultaneously.

Three patterns drive the failures:

- **Siloed workflows.** Security, legal, and eDiscovery professionals operate sequentially rather than concurrently. By the time legal arrives, the security team has already made the decisions that will define the evidentiary record.
- **Unknown retention cliffs.** Default log retention periods on cloud and SaaS platforms create hard deadlines that most legal teams never know exist until the window has already closed.
- **Privilege structures built after the fact.** The engagement structures that protect breach investigation reports under attorney-client privilege must be established before the investigation begins. They cannot be created retroactively, and they are frequently overlooked in the urgency of active incident response.

THE PATTERN: These are not failures of competence, but failures of timing and coordination. The practitioners most exposed are often those with strong eDiscovery fundamentals who have simply never encountered a matter where the breach and the lawsuit were the same event.

WHAT DEFENSIBLE RESPONSE LOOKS LIKE

Avoiding these pitfalls does not require extraordinary resources. It requires specific, advance preparation in each of the four areas IST is built to deliver:

A legal hold protocol triggered at breach discovery, not at counsel notification. IST's team engages alongside the security team from the first hour, establishing hold obligations before remediation begins.

A cloud and SaaS log retention audit, conducted before an incident occurs. IST's pre-engagement data mapping identifies every platform, its default retention window, and what must be extended or preserved immediately.

Pre-structured forensic vendor engagement, with outside counsel directing the engagement and the retention letter in place before the investigation begins. IST's standard engagement structure is designed to support privilege from the first document.

A cross-border data transfer analysis completed before collection, not after. IST's Global Digital Forensics team conducts this analysis as a standard component of any matter involving non-U.S. data.

The organizations that manage the legal dimensions of a breach most effectively are not those with the fastest technical response. They are those who treated the legal dimensions as preparation requirements and who had a partner ready to execute them, not crisis management tasks.

THE CASE IS BUILT
IN THE FIRST 72 HOURS

The evidence that exists when litigation arrives is a direct product of decisions made in the first hours of incident response. Logs preserved or lost. Systems imaged or rebuilt. Privilege structures established or improvised. Notifications drafted with legal strategy in view or without it. Every one of those decisions is either an asset or a liability by the time the first discovery request arrives.

IST Discover-E exists precisely for those 72 hours and everything that follows. Our forensic and eDiscovery team is built to move at the speed of an incident, document at the standard of a courtroom, and stay with the matter from first response through final production.

13+
YEARS AVG. EXPERIENCE PER IST PROJECT MANAGER

24/7
AVAILABILITY — 365 DAYS A YEAR

AM LAW 100
WHERE IST'S PMS ARE SOURCED FROM

SOC 2 TYPE II
US-BASED HOSTING CERTIFICATION

$1.75M won for a law firm through rapid processing, precision culling, and expert PM oversight.
50% review time reduction for a national litigation firm via case consolidation in Relativity.
97%+ data volume reduction achieved through AI-assisted culling before human review begins.

When a breach becomes a case, the question is not whether you had a forensic vendor. It is whether you had the right one who was already engaged, documenting, and building the record that wins.

A Note on Sources: The scenarios described in this paper are drawn from published litigation, regulatory proceedings, and patterns observed across the eDiscovery and forensics practice. Specific case citations are available upon request. This paper does not constitute legal advice.

Greg Caraway
Vice President, Legal Solutions
IST Management Services

404.394.4166
gcaraway@istmanagement.com