

JANUARY 21, 2026 | PUBLICATION

"Preserving Privilege in Cyber Incident Response: What Recent Cases Teach and How to Structure Investigations from Day One"

Counsel and incident responders know the first 72 hours of a cyber incident are unforgiving. In the rush to triage, remediate, and notify, organizations can lose sight of a critical objective: preserving attorney-client privilege and work-product protection over core elements of the investigation. That oversight can be costly. Non-privileged communications and reports are prime targets for regulators, private plaintiffs, and shareholders, and, if disclosed, can complicate defense strategy and harm reputation. The goal is not to hide adverse facts; rather, privilege enables candid legal analysis and protected deliberations, which are then too easily taken out of context when exposed in discovery. Courts continue to scrutinize privilege claims over incident response materials, but organizations that structure their investigations correctly from the outset significantly improve their odds.

This article synthesizes the latest trends and case law and offers practical guidance to maximize privilege over forensic reporting, legal advice, and related communications, without impeding operational response.

INDUSTRY SECTOR

Technology

SERVICE LINE

Technology, Data Privacy, Cybersecurity & AI

RELATED PROFESSIONALS

C. Jade Davis

MEDIA CONTACT

Wendy M. Byrne

wbyrne@shumaker.com

The Doctrinal Baselines: Privilege, Kovel, and Work Product

Attorney-client privilege protects confidential communications between clients and lawyers made for the purpose of obtaining or providing legal advice. Under the Kovel doctrine, that protection can extend to third-party specialists—such as forensic firms—whose involvement is necessary for counsel to render legal advice.

Work-product protection applies to documents and tangible things prepared in anticipation of litigation. Courts increasingly probe whether an incident response report would have been prepared in substantially the same form in the ordinary course of business. Where a report's "true objective" is business or technical, or where it mirrors pre-incident scopes of work, courts are less likely to find protection. Dual-purpose documents can still be protected in some jurisdictions, but the predominant purpose and the but-for causal link to litigation are under close scrutiny.

Structure the Investigation for Protection: Six Core Practices

1. Outside counsel should retain and direct the forensic firm for each distinct incident. Organizations should avoid engaging an existing business-as-usual vendor for incident response under the same master services agreement or scope. Best practice is a separate, outside-counsel-retained engagement specific to the incident, with a scope that ties the work to legal advice and anticipated litigation. Courts have rejected privilege where the vendor's scope did not materially change after counsel became involved or where only the reporting channel—not the work itself—shifted to counsel.
2. Be strategic about the form and content of incident reports. Reports that read as operational or technical artifacts are less likely to be protected. Limit business remediation recommendations in counsel-directed memoranda; where operational guidance must be shared, consider separate "tear sheets" or executive summaries for business stakeholders. If multiple documents are prepared, ensure they are genuinely distinct in purpose and content to avoid subject-matter waiver across workstreams.
3. Anticipate federal disclosure risk and plan for Rule 502. Intentional disclosure in a federal proceeding or to a federal agency can trigger broader subject-matter waiver. In-house counsel should carefully weigh the benefits of sharing privileged material with regulators, consider targeted confidentiality agreements, and, where feasible, seek a Rule 502(d) order limiting waiver. Reports prepared primarily to satisfy regulatory compliance, as opposed to litigation, are less likely to be protected. Where possible, document the dual purpose and tie legal work product to counsel's mental impressions and litigation strategy.
4. For multinationals, prefer external counsel as the privileged gateway overseas. In several non-US jurisdictions, communications involving in-house counsel are not privileged. International investigations should therefore route investigative communications through outside counsel to preserve privilege across borders.
5. Invest early to avoid costly fights later. A modest upfront effort to align retention strategy, scopes of work, reporting formats, distribution controls, and budget sources pays dividends when litigation or investigations follow. Treat privilege preservation as a first-order workstream alongside containment and remediation.
6. Coach teams to write for the record. Even when privilege likely applies, there is no guarantee. Encourage clear, factual, and restrained written communications, avoiding speculation, hyperbole, and casual commentary. Preserve relevant materials, but favor counsel-led oral briefings for the most sensitive legal analysis.

Factors Courts Weigh—and How to Align Your Playbook

Courts look beyond labels to how the investigation was actually run. They examine who retained the vendor;

whether the vendor's scope differed from ordinary-course services; who paid; whether there were dual tracks; the scope of distribution; how the report was used; and whether the work product reflects counsel's legal strategy. The following themes recur:

- Relation to vendor's ordinary work. Where the incident response scope mirrors prior consulting or managed services work, courts find the report would have existed even absent litigation. Distinguish the incident engagement through a separate agreement, a materially different scope, and deliverables designed to inform legal advice.
- Budget source. Payment from legal budgets supports the position that the work was for legal advice and in anticipation of litigation. Business-critical or IT cost centers weigh against protection.
- Dual-track investigations. A clean separation between a business continuity track and a counsel-directed legal track can strengthen protection—if both tracks operate independently and the privileged track focuses on legal exposure and strategy. Dual-track in name only will not suffice.
- Distribution and use. Broad internal sharing—to boards, large cross-functional groups, regulators, or third parties like insurers or law enforcement—undermines privilege and work product and can lead to waiver. Circulate need-to-know legal memoranda while providing business stakeholders with separate, non-privileged updates.
- Content and format. Reports heavy on technical findings and remediation recommendations read as business documents. Counsel-directed memoranda that integrate forensic learnings into legal analysis and litigation strategy are stronger candidates for protection.

Recent Decisions: Patterns and Practical Implications

Courts have increasingly required production of vendor reports where the investigation appeared business-driven, where scopes mirrored pre-incident work, or where distribution was broad. At the same time, opinions continue to recognize protection when companies implement a genuine counsel-directed track focused on legal advice and litigation preparation.

Case	Outcome	Core Rationale	Practical Lessons
In re Target (2015)	Privileged/work product	Dual, independent legal track; narrow distribution; legal purpose	Stand up a counsel-directed track that is genuinely separate from business response.
In re Experian (2017)	Work product	Vendor work and deliverables directed by counsel; report form tied to litigation	Ensure the hot-for link to litigation and deliver to counsel in a legal-advice format.
In re Firearm (2017)	Not protected	Scope unchanged from ordinary course	Use a new, incident-specific scope distinct from pre-incident work.
Dominion Dental (2018)	Not protected	Business-oriented purpose and scope	Avoid ordinary-course language and operational focus in the engagement and report.
Capital One (2020)	Not protected	Pre-existing M&A; business budget; broad distribution; single track	Separate contract, legal budget, narrow distribution, dual tracks.
Quo Wengui (2021)	Not protected	True objective business; broad sharing; no functioning dual track	Ensure legal track has substantive work; avoid wide external sharing.
Butter's (2021)	Not protected	Engagement framed as business/IT monitoring; no litigation purpose	Draft scopes to tie to legal advice and anticipated litigation.
Samsung (2024)	Not protected	Significant business purposes; broad dissemination	Limit distribution; avoid business-wide reliance on counsel-track analyses.

Courts have also cautioned that disclosing one report can waive protection over related materials by

revealing the goals, scope, methodology, and findings of the investigation. Where multiple documents exist, clearly delineate their purposes, audiences, and contents. Notably, some courts have upheld protection over counsel-directed memoranda reflecting legal analysis while requiring production of technical update decks and findings.

Practical Guidance: Building a Defensible Privilege Framework

- Engagement architecture. Have outside counsel retain the forensic firm on an incident-specific engagement. Avoid using the same master agreement as ordinary-course services. Define deliverables as legal-advice inputs and litigation preparation, not operational remediation.
- Scope discipline. Ensure the scope meaningfully differs from pre-incident work and avoids business-as-usual tasks. If the same vendor is used for both proactive and incident work, maintain separate agreements and clearly distinct scopes.
- Where feasible, pay incident response legal-track fees from the legal budget. Document that retention was driven by anticipated litigation and the need for legal advice.
- Dual tracks. Run a business continuity/remediation track in parallel with a counsel-directed legal track. The legal track should gather facts for legal analysis, not manage day-to-day remediation. Keep workstreams and deliverables separate.
- Report design. For counsel-track work, prefer attorney-authored or attorney-integrated memoranda that incorporate forensic inputs into legal assessments. Reserve technical slide decks and remediation recommendations for the business track.
- Distribution controls. Circulate counsel-track analyses on a strict need-to-know basis. Use tailored summaries for broader business audiences to avoid distributing privileged documents. Carefully consider whether, when, and how to share with regulators, insurers, auditors, and law enforcement.
- Communications hygiene. Mark materials appropriately, but do not rely on labels alone. Encourage precise, factual communications and prioritize oral briefings with counsel for sensitive topics.
- Rule 502 planning. Before sharing with federal agencies, evaluate waiver risks and consider confidentiality agreements and, where appropriate, seeking a Rule 502(d) order to limit subject-matter waiver.
- Cross-border considerations. In jurisdictions that do not recognize in-house privilege, ensure outside counsel directs and channels investigative communications.

Incident Response: A Practical Playbook for Counsel

- At detection, engage outside breach counsel immediately to retain and direct the forensic firm under an incident-specific agreement. Route scoping, work orders, and reporting through counsel.
- Stand up a dual-track model: a business continuity team for restoration and regulatory notifications, and a legal track that gathers facts for legal exposure analysis and litigation strategy.
- Define deliverables for the legal track as attorney work product, memorialized in counsel's memoranda incorporating forensic findings, rather than a stand-alone vendor "report" designed for broad operational use.
- Institute a distribution plan: legal memoranda limited to the litigation team and essential executives; business updates via separate summaries that do not reveal counsel's analysis or privileged content.
- Maintain a privilege log strategy from day one and anticipate requests from regulators and private plaintiffs; prepare to defend the investigation structure, budget source, and purposes.

Bottom Line

Courts are probing how organizations actually conduct their post-incident investigations. The strongest privilege and work-product positions arise when companies can show that outside counsel retained and

directed a distinct investigative track whose outputs are tailored to legal advice and anticipated litigation, that business stakeholders received separate operational communications, and that distribution and budgeting reflect a genuine legal purpose. An ounce of preventative structuring at the outset can make the difference between preserving core protections and handing adversaries your playbook.

Please contact Jade Davis or a member of Shumaker's Technology, Data Privacy, Cybersecurity & AI Service Line with questions or for more information.