Articles + Publications | February 20, 2026

FirstEnergy and Your IR Team: Structuring Expert Involvement to Preserve Privilege

This article takes the next step and focuses on what businesses can do before an incident to structure their vendor relationships and IR plans in alignment with these key legal lessons. We focus on four core IR vendor types: digital forensics vendors, restoration vendors, public relations (PR)/communications firms, and data mining/data review vendors.

WRITTEN BY

Sadia Mirza | Timothy J. St. George | Kaitlin J. Clemens

This article was originally published on The Legal Intelligencer *and is republished here with permission as it originally appeared on February 20, 2026.*

Introduction: From Legal Framework to Practical IR Teams

This is the second article in a three-part series on FirstEnergy and incident response (IR). In the first article, **"**FirstEnergy and Incident Response: Preserving Privilege in Cyber Investigations," we walked through four key legal lessons from the U.S. Court of Appeals for the Sixth Circuit's decision in *In re FirstEnergy* and how they apply to cyber investigations, including:

- Engaging counsel at the outset of the investigation;
- Ensuring counsel meaningfully directs the investigation;
- Recognizing that dual legal and business purposes do not automatically defeat privilege or work product protection; and
- Understanding that sharing information with "friendly" third parties does not automatically waive the attorney-client privilege and work product protections.

This article takes the next step and focuses on what businesses can do before an incident to structure their vendor relationships and IR plans in alignment with these key legal lessons. We focus on four core IR vendor types: digital forensics vendors, restoration vendors, public relations (PR)/communications firms, and data mining/data review vendors.

Digital Forensics Vendor

Digital forensics (DFR) vendors are often one of the first external experts engaged in a cyber investigation. Their objectives typically include ensuring the incident has been contained and the bad actor is no longer in the system; identifying the root cause of the incident; and determining what the threat actor may have done or taken while in the environment.

Viewed through the lens of *FirstEnergy*, a carefully structured DFR engagement can strengthen the argument that investigation qualifies for attorney–client privilege and work product protection. The engagement should be designed to promote open and candid dialogue among the DFR vendor, the business, and counsel, so that underlying nonprivileged facts helpful to the investigation can be fully surfaced. At the same time, those discussions may touch on potentially damaging context—such as the rationale for not implementing a particular security control, beyond the simple fact that it was not in place.

Although the underlying facts (e.g., indicators of compromise or the presence of malware) themselves may not be protected, there can still be sensitive communications about those facts that businesses will want to keep privileged. To best preserve these protections, it may be advisable to handle such discussions verbally and in consultation with counsel, so they directly inform the provision of legal advice.

FirstEnergy highlighted that privilege and work-product protection turn not just on using a vendor, but how that vendor is engaged and used in the investigation. To apply these lessons before an incident occurs, businesses should consider:

- How are DFR vendors currently engaged by the business—through the security team (for example, via a retainer) or at the direction of legal—and has the organization considered whether that approach supports counsel's role in directing and relying on the investigation?
- Is the security team aware of legal's role in engaging and directing DFR vendors, and do they know who to contact and when if an incident arises?
- What is the process for requesting, drafting, reviewing, and distributing forensic reports (including who receives them and in what form), and is that process designed to support applicable privilege and work-product protections?

The initial stages of an incident move quickly—often within hours of discovery. Having clear answers to these questions in advance will help to reduce the risk that businesses will be trying to figure out "who do we use and how do we engage them" in the middle of a crisis.

Restoration Vendor

Restoration vendors' are typically tasked with rebuilding and hardening affected systems, restoring backups, and helping resume business operations safely. They may be engaged directly by IT or operations, operate as a separate workstream alongside the forensic vendor, or serve as a subcontractor dedicated solely to restoration. Under *FirstEnergy*'s framework, however, even activities such as these that may appear purely operational can carry significant legal implications. Restoration-related decisions, such as what to restore, in what order, on which systems, and using which methods, can directly affect the preservation of evidence and logs, the integrity and completeness of the forensic record, and the organization's ability to satisfy regulatory or contractual obligations (including notice, reporting, downtime, data retention, and mitigation requirements). As a result, restoration planning and execution should be coordinated with legal and forensic teams to help ensure that business recovery efforts do not inadvertently compromise evidence or undermine the company's position in anticipated litigation, regulatory inquiries, or contractual disputes.

Against that backdrop, similar considerations arise for how organizations structure and document their

communications with restoration vendors.

As with DFR vendors, open and candid communications are important to accurately understanding the underlying facts and technical decisions, but businesses may not want those strategic discussions to be discoverable. To best protect the legal posture around a vendor's restoration work, businesses should consider:

- Does the business currently have a restoration vendor on retainer, and if so, how might that arrangement affect the argument that the vendor's work is part of a counsel-directed legal investigation? Having a vendor on retainer is not inherently problematic, but when legal is the driving force behind the engagement, additional steps, such as clearly documenting counsel's direction, scoping the work in legal terms, and channeling communications through or at the direction of counsel, may be advisable to support privilege and work-product arguments.
- How will the organization ensure that forensic findings are shared with the restoration vendor in a manner that is deliberate, limited to what is necessary, and consistent with maintaining applicable legal privileges and protections?
- Is there a clear process requiring the restoration vendor to consult with counsel or the forensic team before taking steps, such as wiping, reimaging, or rebuilding systems, that could affect the preservation of evidence or logs, and are those decisions appropriately documented?

Public Relations

Incidents often result in media attention and how you manage communications directly affects potential legal exposure and regulatory scrutiny. Additionally, what you say, who you say it to, and when, will also affect potential legal exposure, and those statements will often be carefully scrutinized later in litigation for any purported misrepresentations. Accordingly, businesses often engage public relations (PR) firms to help craft strategies with the legal issues in mind. They often assist with drafting public statements, FAQs, website content, and media responses, and advise on messaging to customers, investors, employees, and other stakeholders.

FirstEnergy supports a structure in which counsel may share factual information with aligned third parties, such as PR firms, without automatically waiving privilege or work product protection over legal analysis and strategy. Even if privileged information is shared, the *FirstEnergy* Court emphasized that work product protection is more likely preserved where the recipient is not an adversary, is contractually bound to maintain confidentiality, and is aligned with the company's interests—circumstances that typically describe a third-party PR or communications vendor.

Although publicly shared communications that a PR firm helps develop may not be privileged, businesses still have key considerations in protecting the underlying strategy and planning that go into crafting those statements.

- Has the organization considered structuring the PR firm's engagement in a way that helps clarify the PR firm's role in supporting legally informed communications?
- Are there clear confidentiality obligations and communication protocols in place (e.g., NDAs, limited distribution lists) to ensure that sensitive factual information, legal strategy, and draft messaging shared with the PR firm are protected and not disseminated more broadly than necessary?
- Is there a defined process for drafting, revising, and approving public statements, FAQs, website content, and press releases that ensure legal review at appropriate stages and creates a defensible record of how key messaging decisions were made?
- Is the organization maintaining a clear separation between internal legal/strategic discussions and the final public statements, so that privileged analysis and risk assessments are not embedded in materials that are

intended to be shared externally?

When structured properly, a PR engagement allows the company to weave legal strategy into its incident-related communications so that they do more than address PR and reputational concerns – they also thoughtfully manage legal risk. Done right, this approach helps ensure that the underlying legal analysis and strategy discussions remain protected, even as the organization communicates effectively with external audiences.

Data Mining Vendor

Data mining vendors play a specialized role in incident response. Their core task is to analyze the data potentially implicated in an incident to determine whose information may be involved and to what extent (for example, name, date of birth, or other identifiers). Counsel then relies on these findings to determine which breach notification laws are triggered, who must be notified, and by what deadlines. The same analysis also informs counsel's assessment of the incident's potential litigation and enforcement risk.

Whether particular data elements constitute protected health information (PHI) or personally identifiable information (PII) under specific laws is ultimately a legal question, but one that depends heavily on the vendor's technical analysis. As with the law firm's work in *FirstEnergy,* a data mining vendor is doing more than simply collecting or transmitting raw facts; it is assembling and structuring those facts so that counsel can answer legal questions about notification requirements and potential liability. In practice, the data mining workstream often combines the organization's institutional knowledge of its data environment, the forensic team's findings, and counsel's legal analysis into a single, integrated effort.

To better position this work for privilege and work-product protection, businesses should consider:

- How are data mining deliverables that may reveal legal strategy—such as search term protocols, data dictionaries, and lists of identified or potentially affected individuals—being drafted and shared?
- Is counsel taking the lead in translating the data mining vendor's technical outputs into legal conclusions about the scope of notification, as well as broader strategy and risk assessments for potential litigation and regulatory inquiries?
- What is the organization's process for sharing—and limiting the sharing—of data mining outputs so that counsel's legal analysis remains protected, while necessary factual information can still be provided to vendors, internal teams, and other external parties to support the response?

Managing the Whole IR Expert Ecosystem Under 'FirstEnergy'

A core element of incident response is not just engaging the right experts, but coordinating their work in a way that consistently applies legal principles like those articulated in *FirstEnergy*. That coordination cannot be improvised in the middle of a crisis. Training and tabletop exercises are practical tools for testing how, in real time, the organization escalates issues to counsel, routes requests for forensic, restoration, and PR support, and documents the legal purpose of those engagements. Well-designed exercises also help teams spot where privilege might inadvertently be put at risk—for example, through informal email threads, broad distribution of forensic findings, or unclear roles for outside vendors—and allow the organization to refine playbooks, engagement letters, and communication protocols before those weaknesses are exposed during an actual incident. By building these practices into routine preparedness activities, businesses can strengthen both their operational response

and their ability.

Sadia Mirza, *a partner with the Troutman Pepper Locke, leads the firm's incidents + investigations team, advising clients on all aspects of data security and privacy issues. She is the first point of contact when a security incident or data breach is suspected, and plays a central role in her clients' cybersecurity strategies.*

Tim St. George,*a partner with the firm, defends institutions nationwide facing class actions and individual lawsuits. He has particular experience litigating consumer class actions, including industry-leading expertise in cases arising under the Fair Credit Reporting Act and its state law counterparts, as well as litigation arising from data breaches.*

Kaitlin Clemens, *an associate based in the firm's Philadelphia office, handles ransomware and data extortion cases, and advises on compliance with state and federal laws, including HIPAA, FERPA, and GLBA, as well as development of privacy programs and pre-incident response strategies, as well as creating and delivering comprehensive training for attorneys who are new to cybersecurity.*

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber