NOVEMBER 22, 2019

Legaltech® news

ONLINE

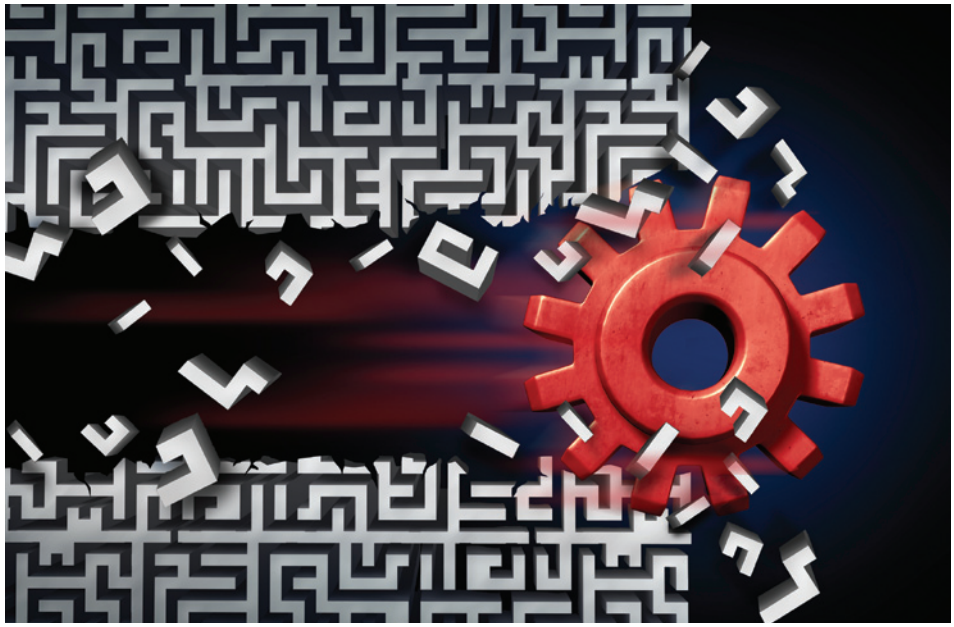
An ALM Publication

Crisis Control: Best Practices for Emergency E-Discovery and Incident Response

A set of steps and best practices that legal teams can follow to ensure thorough and efficient handling of e-discovery in crisis situations.

BY ANDREW JOHNSTON, FTI CONSULTING

*This article appeared in **Cybersecurity Law & Strategy**, an ALM publication for privacy and security professionals, Chief Information Security Officers, Chief Information Officers, Chief Technology Officers, Corporate Counsel, Internet and Tech Practitioners, In-House Counsel. Visit **the website to learn more**.*



Credit: Lightspring/Shutterstock.com.

The day the mine collapsed in the Atacama Desert, the world held its breath. Across time zones and over months, we watched in simultaneous disbelief and hopefulness as rescuers worked to reach the men trapped below. As humanity does in all major crises — energy plant explosions, oil spills, commercial fires — we shared in awe and concern at the first responders working to save lives and contain the damages. In these emergencies, what most don't recognize is that the events span far beyond first response on the ground. Behind the scenes, and long after the news cameras stop rolling, a separate set of teams are triggered, preparing for and managing the extensive legal and investigative processes that follow.

Under the intense emotion and stress inherent in crisis circumstances, legal teams orchestrate short term e-discovery to uncover who knew/knows what relating to the crisis and events leading up to and immediately following it. They assess the breadth of damage and injury in the moment as the crisis unfolds, alongside launching longer-term investigations into what caused the accident and any potential negligence or wrongdoing that occurred. Getting to the facts quickly is critical to prepare for litigation, government investigations and potential criminal charges, and to expedite restitution for victims.

Our teams have worked on a number of crisis e-discovery matters around the world, supporting clients through the lifecycle of complex investigations and litigation that result from these disastrous and often tragic events. In most cases, crisis e-discovery projects are highly likely to involve large data volumes (often double digit terabytes) and span many involved parties (*e.g.*, a committee of plaintiffs of affected parties, governmental agencies, foreign governments, states' attorneys general, etc.). They require tremendous manpower and broad expertise in all practice areas, including data collection, processing, project management, advanced analytics, case management, foreign language review and production. Timelines are often extraordinarily tight, especially in government investigations in which counsel is preparing for congressional testimony and other regulator requests for data.

Another complicating factor is a common desire to collect and review text and social media communications, which can be more prevalent in crisis situations than in other types of cases. When disaster strikes, people

today often send a text, chat message or interoffice IM. Investigations may sometimes reveal communication that someone intended to be "off the record," which may provide important insights into the facts of the case.

Best Practices

Through our work with these types of matters, our teams have learned some important lessons. Drawing on these, we have established a set of steps and best practices that legal teams can follow to ensure thorough and efficient handling of e-discovery in crisis situations. These include:

Don't panic, develop a plan: The legal team will be pulled in many different directions, so it is critical for them to take a step back and breathe. This will create space to think carefully about the matter. At this point, it is important to ask questions to understand what will be most important downstream, the full scope of data sources that need to be considered, how they may need to be shared among multiple team and all potential pitfalls that may arise. Counsel should also build a plan for garnering information from key stakeholders, and begin interviews to determine all areas where data may live and all owners of important data.

Rally a strong team: A strong team that can support every facet of the crisis, end-to-end, is essential. This should include a strategic communications team that can develop a clear narrative about what happened, and distribute that information across shareholders, employees, board members and the media. Also bring in experts that can investigate the situation from a regulatory perspective, remediate compliance issues and interface with regulators. A cohesive team that works together across all areas will ensure efficiencies as the crisis continues to evolve, and help maintain a smooth path forward. In one recent matter, consultants from across our organization supported a client in a major crisis — the e-discovery team was mobilized, and in parallel the strategic communications and investigations teams collaborated with the law firm to align on the risk exposures and the details that needed to be communicated to stakeholders and regulators.

Preserve carefully: It is important for relevant data — from computers, mobile devices, hard copies, USB drives, key data systems (such as rig information units for offshore oil, or research data for a product liability case) and other sources — to be preserved for potential use downstream. This doesn't necessarily mean the team must review it, but it needs to be available. Take care to confirm that nothing is "lost," to avoid adverse consequences or inferences made during a proceeding.

Be strategic about unconventional data types: Consider whether text messages, chat strings, voicemails and other communications may come into scope given the particular context. These files can sometimes be looked at together to develop a timeline for a particular actor or group of people. Teams may need to look for documents (not just text messages) saved on mobile devices, and find back-ups when possible. Individuals will often back up their phones to their computer or the cloud, and data will remain there until removed. Gathering iterative back-ups may in some circumstances help fill in the chain of events. Further, forensic experts can help counsel dig into databases of texts to identify gaps in the messages listed in the database to help fill in blanks that may have been created by deletion.

Identify important information: Right away — or better yet in advance of a crisis — a plan for identifying critical information should be put in place. This will allow the team to begin processing for analysis and quick fact finding ahead of investigatory inquiries. One piece of this is to have insight into the key stakeholders that pertain to each piece or set of data and a method by which to track who was issued which device. As early in the process as possible, interview the key stakeholders and determine others who may have more "on the ground" knowledge of how something was used, where data was saved, etc., in the course of business.

Enable agility: Things can change quickly in these matters, and counsel needs to be prepared to endure the changing tides of the investigations and litigation. Working with outside experts that can provide on-the-ground support is key. This provides collaborative support and experienced backing for the teams dealing with the actual crisis. A general best practice is for the in-house team and all outside providers to maintain frequent touchpoints with each other, regulators and opposing counsel to keep things moving forward smoothly.

Lawyers that have experienced these situations, or those that work within industries subject to major accidents, know that emergencies require them to mobilize quickly. Without an effective plan, counsel will find it much more difficult to bear the stress and emotional strain of the ordeal, which can lead to trickle-down implications for the company, its partners and the people impacted by the crisis. But following a playbook of key steps can make a big difference in ensuring everyone stays calm, gathers as much information about the incident as possible and is able to respond in a timely way.

Andrew Johnston *is a Senior Managing Director in the Discovery practice within the Technology segment at FTI Consulting. As an expert in e-discovery technology, he helps clients across the lifecycle of the discovery process, including the review and production of electronic data. He is based in Wayne, PA.*