Deloitte.

Responding to Large Scale Litigation
Post incident game plan

Organizations which may have limited experience with large scale litigation within the United States are faced with significant hurdles when dealing with the identification, preservation, collection, review, and production of materials responsive to government inquiry, third party requests, and plaintiff requests for production. These issues can be exacerbated when dealing with a situation that couples the need for crisis management with estimating future litigation and investigatory demands.

Understanding and appraising the myriad of complex preservation obligations from the outset of the incident, to the response effort, and finally the litigation cycle, can provide an organization with a host of opportunities to develop and institute a defensible process to reduce downstream document collection, review, and production costs, decrease potential fraud, and ultimately protect shareholder value. The circumstances of the litigation response effort should be carefully balanced with need for business continuity of operations.

Organizations, in concert with their legal teams and consultants, should consider focusing on the following core areas during the first ninety days post incident and into the response effort:

Establish a multi-disciplinary Core Team: At the outset, organizations should assemble a Core Team to spearhead and tackle the various competing demands of the incident, the post incident response effort, the internal investigation, and prepare post incident plans of action to mitigate future incidents. The team should be comprised of individuals with subject matter specialization and include individuals from internal legal, external counsel, consultants, internal audit, IT, HR, regulatory affairs, finance, risk, and compliance. Each member of the Core Team should lead a smaller team responsible for their specific function. The Core Team should meet regularly to share information from their respective vantage points and to provide status updates to the C-suite. This Core Team should also coordinate efforts among their respective external counterparts to facilitate effective transfer of information and deliver on an agreed upon and aligned strategy by all stakeholders.

Identify Potential Data Sources: The immediate identification of custodial and noncustodial data sources within and external to the enterprise is critical. This may include traditional sources such as laptops, hard drives, mobile devices, mail servers, accounting systems, HR applications, instant messaging applications, voicemail servers, etc. In addition to traditional sources, organizations should consider nontraditional sources such as social media, third party or private cloud systems, eRooms, SharePoint sites, third party systems and communication vehicles, etc. Data may also derive from a number of custodial sources in addition to company employees, such as third party contractors, vendors, experts, technicians, members of the board of directors, government organizations, etc. Once potential data sources have been identified, a data map should be constructed, which should include a methodology for gathering information about the data sources from custodians and IT system owners through electronic surveys or interviews.

Preservation of Data: Once data sources have been identified, steps should be taken to preserve potentially relevant data whether internal or external to the organization. Legal hold notices should be cascaded to individuals within the organization with potentially relevant information and those who may control non-individual data sources which may contain potentially relevant data sources. It is presumed that every custodian and/or system identified will not have data harvested from it, but at the onset, it is better to over-preserve than under-preserve. Similarly, preservation notices may be sent to contractors and vendors which may possess potentially relevant information. Legal and IT should play a key role in examining existing retention policies against legal hold obligations, and adjusting designated system-wide auto-delete, auto-archive, or other automated data deletion functions. It is important to consider how the organization provisions mobile devices and the retention of data from these devices due to the limited ability of mobile devices to retain data for long periods of time. Backup systems should be promptly investigated, and an extended retention schedule for backup tapes should be instituted as soon as possible.

Plan for Separating Employees: HR and IT should develop a plan to mitigate the loss of data through the loss of employees, either voluntary or involuntary, during the normal operation of the business. This plan should constitute the interviewing of custodians who were identified as having data which may be potentially responsible prior to separation, the collection of physical custodial assets such as a laptop and phone, the collection of network assets and voicemail, and should include a plan for the provision of assets to new employees once the data has been captured to reduce IT costs during the litigation cycle. Should unexpected immediate separation occur a plan should be created to identify managers who should be interviewed about employee involvement in the incident or post response effort.

Plan for Decommissioned IT Assets: IT and finance should develop and execute on a plan to account and preserve decommissioned IT assets during the normal course of business operations. It is important to understanding lease expiration dates of assets in the enterprise so that a preservation schedule can be put into effect prior to taking these assets offline. Organizations typically have planned upgrades and schedules, and with care, these should be able to continue.

Acquisition and Tracking of Data: The Core Team should work with its outside legal counsel and vendors to establish leading practices around the forensic collection of and tracking of data sources. This may include the global deployment of forensic collection personnel as well as the use of in-country resources where data privacy is a concern. Consideration should be given to remote forensic collections, manual collections, and mobile device collections, as well as the various collection methods and scope that may be appropriate to individual matters. A data acquisition and tracking strategy should be designed and implemented which is repeatable and defensible. Careful consideration should be given to the tracking methodology for data sources including but not limited to the information tracked and consistent nomenclature. A common database should be used for this effort to help ensure that all information about the data is in one place and can be easily searched, sorted, and reported upon at the request of legal teams. The tracking of non-collected data sources is just as important as the tracking of collected data sources, and consideration should also be given to the tracking of data sources that are being "retired" or "demobilized." Establish data source repositories as needed, implement bar coding systems for collected devices and implement secure data device storage areas (physical and virtual "evidence rooms"). In addition, the legal team and the forensics vendor should establish clear chains of custody processes and consistent forms along with the establishment of digital evidence records, keeping in mind that teams may be collecting in the field.

Processing and Hosting Data, and Managing Data/Document Review: Data should be collected and processed on a rolling schedule, and thus a processing, hosting, and document review plan of action should be created at the outset in consultation with inside and outside counsel and the selected vendors. Coordination between the collection, processing, hosting, and review teams is critical to the effective production of data, mitigation of risk, and the reduction of downstream costs. Processing specifications should be constructed at the outset and agreed upon by all stakeholders. Collected data should be reviewed in an efficient and cost-effective manner. Consideration should be given early-on to using one hosting and review platform. Enterprise management of the document review process should be implemented to help ensure consistency across reviews, mitigate risk in inadvertent productions, and facilitate a better understanding of the data. Where specialized outside counsel are employed for different litigations and investigations, one review management team should be considered to provide continuity and context among counsel. Scalability may dictate the use of vendors for large-scale, complex, simultaneous data/document reviews for multiple litigations and investigations. Important consideration should be given to process and review team management. Lastly, newer technologies such as predictive coding should be considered if the selected vendor has knowledge in this arena.

Leading Practices to consider during the initial phase of the response, which can impact success over the long term are:

1. Plan for scalability—and build scalability into each of the below practices
2. Bring the "right" skill-set to key project roles at every level and function
3. Bring the "right" technology to key project processes such as forensic data collection, data tracking and management, processing, hosting, and analytics
4. Define a process for each matter in the continuum and document it and memorialize changes to the process
5. Establish quality controls and data integrity checks for each defined process and enforce them—this can add to the defensibility of the process and mitigate risk
6. Document or log key decisions both project-wide and within matters—this can assist with continuity during long term litigation
7. Establish a communication plan including touch points, project wide meetings, micro-meetings, and meetings with the Core Team
8. Implement an on-boarding, off-boarding, training and cross training program from day one
9. Engage a project management office early-on to standardize billing and expense structures, coordinate project-wide communications, and assist with centralizing key project documentation
10. Build and foster relationships among the Core Team, vendors, and all stakeholders to facilitate a "one team" approach—clearly delineated roles and responsibilities with concomitant accountability will assist in this effort

The importance of being ready to respond to eDiscovery: Experience has shown that a company's ability to respond deliberately and decisively within the first 90 days of an incident or crisis can be critical to the business outcome. Equally as important during this time is the company's legal and management response. Familiarity with all phases of the eDiscovery continuum, employing leading practices from the onset, and deploying a strong discovery management response team in the first 90 days can provide a defensible foundation from which to build on through the long term.

Contacts

For more information, please contact:

Bryan Foster
Director, Deloitte Advisory
Deloitte Discovery
Deloitte Transactions and Business Analytics LLP
bfoster@deloitte.com
+1 713 982 2747

Michael Stanioski
Senior Manager, Deloitte Advisory
Deloitte Discovery
Deloitte Transactions and Business Analytics LLP
mstanioski@deloitte.com
+1 617 437 2234