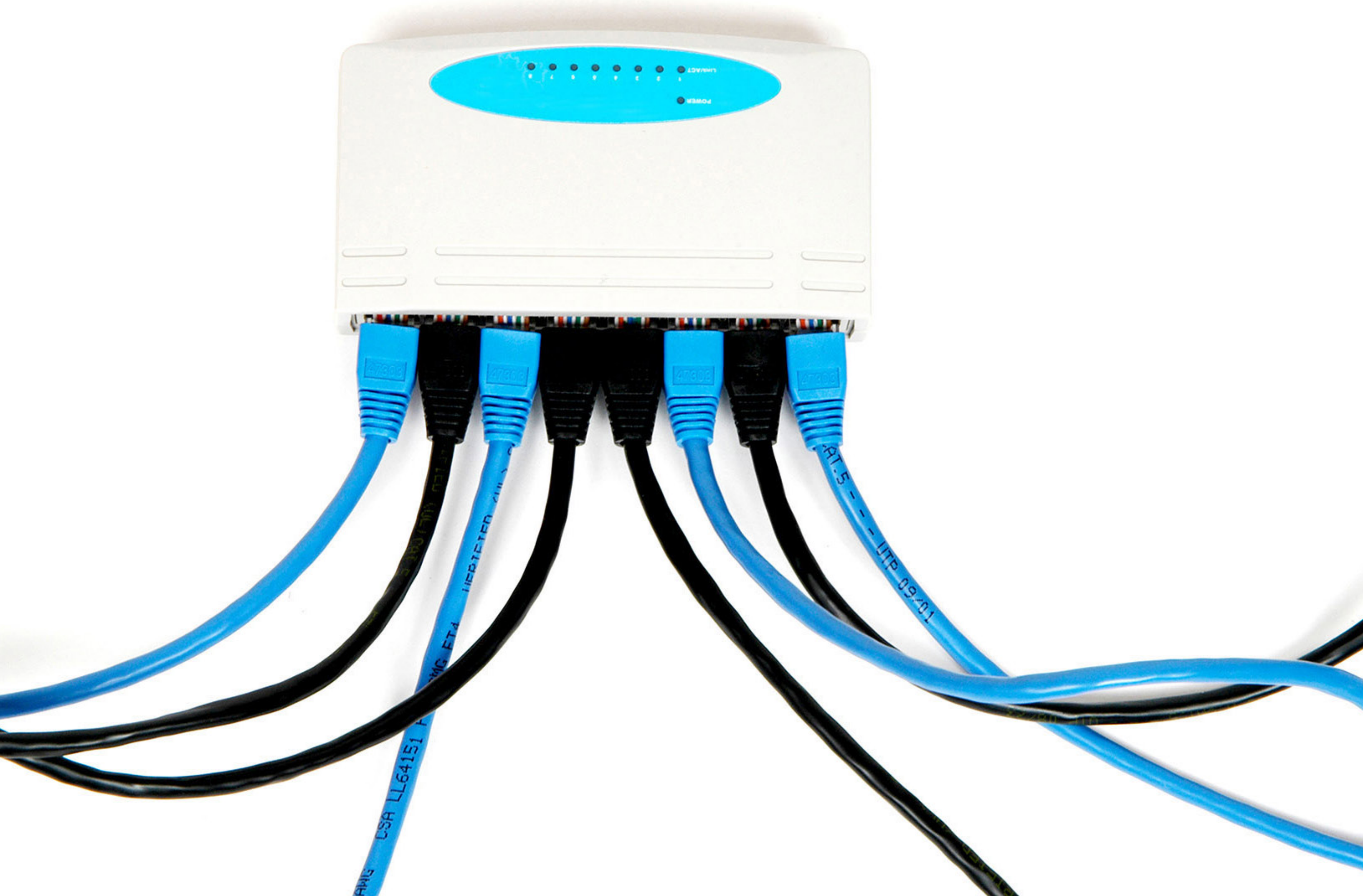
Deloitte.

Bringing eDiscovery In-house
Designing a Playbook for your Organization



Introduction

Over the past few years, in an effort to control the well-publicized skyrocketing increases in electronic discovery costs, a number of companies have responded by bringing portions of their eDiscovery processes in-house. One challenge they face is that eDiscovery is complex and requires specialized knowledge of legal procedures, information technology, and the flow of information within the company. It can also be demanding because courts and regulatory organizations often set tight deadlines and do not accept excuses for being late.

To improve effectiveness, companies should develop and codify a set of procedures into a formal document; an eDiscovery playbook. The playbook's purpose is to create a process that is articulated, predictable, and repeatable so that it is defensible. It should reduce ad-hoc decision-making and help employees understand their roles and responsibilities. Since eDiscovery costs can escalate rapidly and mistakes can lead to sanctions, the rationale for creating a playbook is no different from other investments that companies make to reduce risks and facilitate quality outputs. Companies using these guides should respond more easily and rapidly than those who use a bespoke approach.

This article is intended to help provide practical advice on the development of a playbook. It focuses on how to preserve and collect data when responding to eDiscovery demands which can be a first step to controlling costs. There are a number of other areas including automation, vetting service providers, and approaches to reducing document review costs which a company should consider when taking steps to control costs.

Approach

The first step is to assemble a project team to create the playbook. The individuals in charge of the team should have experience with project management and the documentation of information workflows. They should be assisted by personnel from the Legal, Human Resources, Information Technology, and Records Management departments. Larger organizations should also include representatives from their business units.

The scope of the playbook may vary based on a number of factors. They include the size and geographical distribution of the company, the regulatory environment it operates in, the types of litigation it faces, and the amount of eDiscovery work it chooses to perform in-house.

A good reference is the Electronic Discovery Reference Model (EDRM) which has been widely adopted by the Legal industry. It provides the framework for the eDiscovery cycle and consists of nine phases; four dealing with on-premise identification, preservation, and collection of data (also referred to as the "left-side") and five (referred to the "right-side") that deal with the analysis, preparation, and presentation of data. We suggest that the playbook focus on the "left side" because companies are often involved in those phases; regardless of whether they outsource the work or perform it in-house. In the following sections, we will cover the high-level questions that companies should address when designing the playbook.

Finally, since eDiscovery covers everything from employee investigations to complex litigation it may be difficult to address every situation. A better approach is to develop a realistic target for the first iteration of the document and adding additional situations on future releases.

Data preservation

Failure to preserve data can be one of a company's biggest legal liabilities. The company may get a second chance if it fails to produce, but failure to preserve can lead to fines and court-ordered sanctions. It is the legal department's duty to notify employees of their obligation to preserve whenever a company becomes aware of possible litigation and the playbook should outline the process to make this happen. Addressing the following questions in the playbook can assist the company with identifying and retaining the appropriate amount of data in a systematic fashion.

How is the legal hold communicated?

The company should implement a process that efficiently routes information to the legal department so counsel can decide if a legal hold is required and disseminate the information to the rest of the organization. The process should also include guidelines and examples for the business units when to contact the legal department.

Counsel should communicate the legal hold to the custodians and the individuals responsible for preserving the data by issuing a formal preservation notice. The custodians should acknowledge the preservation notice in writing so counsel can track who received the notification and follow up with custodians who may be away. The preservation notice should also include questionnaires and standardized forms to be filled out by the custodians. The purpose of the questionnaires include targeting the collection, deciding if additional custodians should be included, and refining the search criteria used to cull down the data. Properly done, the questionnaires can provide added confirmation that the scope of the ESI being collected is complete.

What is the covered material?

Counsel should use guidelines to decide what material should be preserved. This includes identifying:

- The time period that applies to the case
- The custodians, the key individuals in the case who possess and control paper documents and electronically stored information (ESI). It may also include the people around them such as individuals who reported to them or to whom they reported.
- Third parties. The use of cloud computing, and outsourcing of traditional business functions means that third-parties may also control information that may be important. In such instances the third-party should also be considered a custodian.
- Categories of data to be preserved including email, electronic files, phone and text messages, data from structured databases such as Sales and Human Resources, and computer backups.

What preservation steps should be taken?

Preservation should involve coordination with the Information Technology department so that potentially relevant data is protected from destruction. The playbook should document the steps to:

- Instruct the Records Management and Information Technology departments to suspend the destruction of paper documents and ESI.
- Suspend the automated deletion of data including email, server backups, and recycling of backup tapes.
- Copy data onto secure centralized locations including email boxes and computer files of custodians.
- Preserve communication from specified custodians using a process called journaling.
- Maintain a master list of the data that was preserved.

With the increasing use of cloud computing and outsourcing of traditional business functions, preservation could also require obtaining copies of data stored at outside service providers. The playbook should include contact information and plans to preserve data at those organizations.

What are the circumstances for reassessing the legal hold?

Circumstances may include additional custodians, changes to the scope of the discovery such as court orders or agreements amongst the parties in the case, and changes to the company's technology. Examples of the latter include upgrading software or decommissioning servers. In those instances, the Information Technology department should notify the legal department and take steps to confirm that potentially relevant data is not destroyed. The playbook should outline possible scenarios and the process to confirm that changes are reviewed by the legal department and communicated to the rest of the company.

The playbook should also document what should be done when a legal hold is lifted. This may include communication from the legal department to the rest company and the procedures to deal with the documents that were held for preservation outside of the company's normal document retention policies.

Data Collection

This section of the playbook should describe the procedures used to identify, copy, label, and document data from the possible sources of relevant data, and follow procedures that preserve its integrity. To do this effectively, the processes should consider the following questions and issues.

What are the potential data sources?

Data may be stored at a number of sources including email, computers, mobile devices, databases, tape backups, and third party sources such cloud storage and cloud backup sites. The group overseeing the collections should review the responses from the questionnaires sent to the custodians and coordinate with the appropriate Legal and Information Technology resources at the company to confirm that all potential sources of data are identified.

What are the appropriate methods for collection?

Methods of collection may include computer imaging, remote collections, as well as assisted and self-collections. There are trade-offs to each approach in terms of efforts, costs, and completeness, but the key is that the process be defensible. For example, computer imaging is more likely to be appropriate for cases involving suspected wrongdoing, whereas self-collections may suffice for regulatory demands or third-party subpoenas. The playbook can serve as a guide to communicate the appropriate collection methods for each instance.

Should the company use internal resources or enlist the help of an outside service provider to perform the collection?

The decision can be based on a number of factors including availability, skillsets and experience of internal resources, expected volume of data, geographic location of data sources, legal and privacy restrictions that inhibit movement of the data, costs, and time (i.e. deadlines for discovery). The company may also consider the importance of the matter and decide to use a certain type of vendor if there is a possibility of sanctions or criminal charges.

Who should be involved in the execution of the collection?

This may include a number of departments within the company as well as outside service providers. Personnel involved in the collection activities should be versed with data handling procedures and Chain of Custody, a process of handling evidence that creates and maintains a transaction record for each individual who assumed or released possession of the evidence. This includes the identification information for media such as computers, servers, and external devices and the date and time they were received. Personnel who handle the media should update Chain of Custody forms at each and every transfer. If not properly performed, it could result in data being rendered inadmissible in a court of law or other legal proceedings.

How to validate the collection is performed effectively the first time?

Because collections can be time-consuming and disruptive, it is important to document on-site quality control procedures to validate that the ESI is properly collected before leaving. A common approach is applying hashing to the original and copied data and comparing the results. Hashing is the process of applying a complex mathematical algorithm to a piece of data such as a file, hard drive, or server that generates an identifier. If the identifiers of the original and copied data match, the pieces of data are considered identical because the odds of two non-identical pieces of data generating the same hash value are remote.

How to control and image computers of departing employees?

Special guidance should be given for the control and imaging of computers for departing employees, especially those who leave on bad terms. There have been instances where evidence was declared inadmissible because the company could not account for the whereabouts of a computer from the time an employee left to the time the computer was imaged. Therefore, it is critical to begin the Chain of Custody from the minute an employee returns a computer.

Checklists, roles, and responsibilities

The playbook should also include templates of standardized communications, notices and checklists that support the steps outlined in the document including:

- **Preservation notices** - outline preservation obligations for computers, PDAs, external devices, software, emails, and paper documents.
- **Questionnaires** - sent to custodians to document the computers, PDAs, data storage devices, backups, emails that they have that potentially holds ESI that needs to be preserved
- **Collections checklists** - steps to follow during a collection
- **Encryption key requests** - requests sent to the Information Technology security staff to obtain encryption keys for computers and devices.
- **Database Collection Forms** – documentation for data exported from legacy computer systems and external providers
- **Chain of Custody Forms** - identify how data was collected and received and who handled it.

The final step is to create a contact list of the personnel who will manage eDiscovery for the company along with their responsibilities and area of oversight. Also, assign coordination responsibility to a project management group (usually aligned with either the Legal or Information Technology departments) to help facilitate timely compliance of the personnel involved.

Rollout and beyond

Once the playbook is finalized, it should be put through a set of mock preservation and data collection exercises to determine completeness, analyze the procedures and identify gaps that may need to be addressed. Rolling out the playbook may range from a high profile campaign to a low-key announcement. Regardless of the approach, be sure to communicate the plan to the appropriate company personnel and gain the support of key stakeholders. Explain eDiscovery, its importance, and why timely response and systematic record keeping are imperative. Also train the individuals who preserve and collect ESI on evidence handling and documentation of Chain of Custody. Although the effort to create and roll out a playbook may take up to several months, the benefits of a well-documented and systematic approach often make this effort worthwhile, given the potential savings in electronic discovery costs.

Management should consider updating the playbook periodically and designating employees with responsibility for its maintenance. The purpose of this exercise is to identify applicable changes to the company's structure and systems and incorporate the changes in the document and to provide the company a chance to evaluate what worked and what did not.

Ultimately, a playbook's effectiveness depends on adherence to the documented procedures and particularly important, systematic record-keeping throughout the litigation cycle. If these actions are followed, the playbook can help the company deal with eDiscovery in a timely manner, promote consistency, reduce the likelihood that important data is overlooked, and make the overall process more defensible. An eDiscovery playbook can lead to lower and more predictable eDiscovery costs and provide the company with a greater sense of security.

For more information

Rafael Lefkovic
Manager, Discovery
Deloitte Financial Advisory Services LLP
+1 212 436 7967
rlefkovic@deloitte.com