5 Key Steps for Collecting Electronic Information

The legal community is beginning to utilize electronic evidence more widely, causing the number of electronic document productions to also increase. As a result, organizations are being compelled to produce electronic evidence however, the processes for doing so are not clearly defined. It can be a difficult, costly, and time-consuming process to collect electronic data such as email communications, Word documents, Excel spreadsheets, and other information that may have been deleted when not done by experienced personnel. The following constitutes steps that may be taken to plan for the collection of electronic evidence:

Step 1: Plan for the Cessation of Data Destruction

Most organizations utilize a form of data destruction or recycling as part of their normal business operations. However, should litigation be pending, it is necessary to cease this destruction, such as disabling email auto-delete features and suspending backup tape recycling, to ensure that relevant electronic evidence is not destroyed. In addition, should deleted files need to be recovered, the hard drives containing them should be immediately forensically duplicated to ensure that deleted files are not overwritten. If litigation is pending involving termination, ex-employee workstations should be archived rather than wiped after their departure.

Step 2: Thoroughly Define the Scope of Information Collection

Once it is clear that electronic information is no longer being destroyed, a clear scope of the collection of information can be delineated.

The following should be identified when defining the scope:

- Who is responsible for managing the relevant information?
- When was the relevant information created?
- Has any of the relevant information been deleted?
- Is any of the relevant information stored on backup tapes or external media devices?

Step 3: Ascertain Potential Sources of Relevant Information

When organizations operate in multiple locations, utilize differing types of technologies, or have employees with disparate access to these technologies, it can be difficult to ascertain where electronic evidence is held. Therefore, it is necessary for legal professionals to collect detailed information regarding the configuration of an organization's information services, which can be done by reviewing existing documentation, interviewing key information technology personnel, and diagramming how relevant information is stored within the organization.

The following will assist with the identification of sources of relevant information:

- What type of email technology, both servers and workstations, does the organization employ?
- Are email messages stored on the email servers or user workstations?
- How often are email messages purged from the servers?
- How are email messages archived and backed up?
- What type of file server technology does the our organization employ?
- Are user files stored locally on their workstations or on a centralized file server?
- Does the organization log the users' file server activities?
- How are file servers archived and backed up?

Step 4: Construct Action Plan for Collecting Relevant Information

After relevant information has been identified, it must then be collected. The information collection action plan should include the following elements:

- An outline of the relevant information sought and potential locations where information resides
- Contact information for necessary internal and external personnel to facilitate the collection of relevant information
- Procedural guidelines for the actual collection of relevant information
- Detailed checklists to be used before, during, and after the collection of relevant information
- Documented chain of custody instructions
- Inventory of forensic tools necessary to facilitate the collection of relevant information
- A summary of anticipated business continuity issues and resolution plans

Step 5: Execute the Collection of Relevant Information

Upon the completion of thorough pre-collection procedures, guidelines, and checklists, the physical collection of relevant information should commence. Organization is critical to ensure all action plans are followed and all procedures are complied with. If problems arise or a deficiency is identified in the action plan, information collection activities should immediately cease in order to address and correct the issues.

Conclusion

To facilitate a smooth litigation and the thorough discovery of electronic information, the importance of a well-orchestrated action plan for the collection of relevant information cannot be understated. Of critical concern is the forensic integrity of electronic information necessitating strict adherence to the procedures for gathering data in forensically sound manners. Additionally, it is vital to maintain a well-documented chain of custody to demonstrate the integrity of collected electronic information has not been compromised and that its whereabouts and ownership can be accounted for. The capability of electronic information to yield powerful electronic evidence is clear however, immense considerations exist, necessitating that the collection of relevant information is performed in a forward-thinking and methodical manner.