Global Information Assurance Certification Paper

IT Guidance to the Legal Team

GIAC (GLEG) Gold Certification

Author: Brad Ruppert, bradruppert@gmail.com
Advisor:

Accepted: April 15th 2009

Abstract

This paper will discuss how an Information Security team should interface with their legal team to ensure both groups remain focused on what they do best. Working with the legal team can often be a drawn-out, overly documented process which might be simplified if they had the right tools and training to gather the information themselves. In today's world e-discovery is a huge component when dealing with any type of litigation so it would be of everyone's benefit that the tool used to collect work-related documents was scalable, easy to use, and intuitive. The goal of this paper will be to provide some techniques for working with the legal team, to recommend areas where Information Technology advice should be provided, and how to make both teams work more efficiently together.

1. Introduction

Technology can be a great tool to simplify a process or increase the output of existing processes. Despite this, Information Technology (IT) teams must be cautious when implementing new technology into their environment because this can also increase their liability of information retrieval if a lawsuit is filed against them. Rarely if ever is an enterprise application, such as e-discovery software, ready to go out of the box. Most enterprise applications of scale require months of planning, negotiations, architecture discussions, engineering consultation, cross-divisional resource allocation, and process redesign to accommodate the software. Information security and IT teams, knowledgeable of this fact should interface with their legal teams prior to ideation of implementing an enterprise e-discovery tool. Just having a tool and not a defined process to effectively manage, correlate, extract, and secure subpoenaed data can leave a company exposed to multiple financial and legal repercussions. An example of this was seen with the case of Morgan Stanley vs. Ronald Perelman where "Morgan Stanley was hit with a $1.75 billion jury verdict, which hinged primarily on the company's lax e-discovery procedures." (Cummings, 2007)

2. Scope

This paper will focus on proactive initiatives that an Information Security team can take to mitigate high risk pitfalls made by implementing an e-discovery solution. It will address the benefits of typical e-discovery technologies and challenges a company may face with their legal teams. It will introduce ideas and strategies to consider when selecting the right e-Discovery solution depending on the nature, size, and flexibility of the business. Selecting a technology solution to fit the enterprise can be a daunting task and should be approached with having a specific goal in mind. Staying informed of the current laws and regulations that govern your business should help provide some guidance as to the processes that need to be implemented. The goal of this paper is to offer some proactive strategies that Information Security teams should consider so as to minimize the impact on their resources in times of litigation.

Brad Ruppert, bradruppert@gmail.com

3. Things to Consider

While it is important to remain aware of the current laws and regulations that govern your business, these should not drive your approach to implementing security controls. Attempting to design a security strategy solely around regulations that govern your business can actually lead to negative consequences. Regulations are often written to address a specific area of concern which may have been developed as a result of a recent judgment or class-action suit. While ensuring adherence to regulations is a must, designing your security strategy around this may leave other critical assets exposed. Regulations should only be a part of your security design and not the primary driving factor as this can "*cause costly and inefficient investments"* in the long term. (Gupta and Sharma, 2008) Security teams should remain focused on their core business model and develop controls that protect their assets accordingly.

Information security managers should spend time developing a close relationship with their legal teams so as to learn their processes and to provide assistance with any information security related challenges. Teams should communicate their roles and responsibilities to one another to understand the various ways they can help in "*answering questions, developing responses to legal inquiries, managing requests for production of digital records needed in investigations, and aiding electronic discovery and digital forensics matters."* (Krause and Tipton, 2006) Information security teams should also dedicate time to reviewing current legislation that governs their business like Sarbanes Oxley or the Gramm-Leach-Bliley Act. The more effort put forth fostering this relationship between information security and legal teams will help reduce process inefficiencies when performing electronic data gathering. Understanding what is required by the law and what the intent of your legal team is trying to accomplish will also minimize time wasted gathering the wrong information.

It is also recommended that information security teams become familiar with lawsuit terns and investigative processes. This will save time and effort when parties exchange requests to produce or gather materials related to a lawsuit. Given the requirements for digital data, opposing legal teams may submit written notice to your counsel requesting the preservation of all artifacts related to their lawsuit. Be certain to

carefully read the details of the request and discuss with your internal counsel so as to fully understand the scope otherwise you may be spending multiple cycles continually going back to retrieve additional information. (Krause and Tipton, 2006) Failure to understand the scope and limitations of this preservation request could have massive legal fines or severely jeopardize the case. It will also help to interface with various IT teams to understand how and where data is stored, transferred, and backed up. During this process understanding, executives and legal teams should be made aware of any potential safeguarding or preservation limitations.

Another key component to keep in mind is that you may be deposed in adversary settings and your actions and records may be subject to questioning. "*As an information security professional, you must act to ensure that you have been diligent in performing your assigned duties to secure and protect digital data in these electronic discovery and forensic matters."* (Krause and Tipton, 2006) It will also be important to ensure that all record keeping is accurate and securely maintained.

4. What is e-Discovery

Electronic discovery (e-Discovery) is a part of the legal process in civil litigation used to gather, maintain, and produce computer-generated information. This can be more cumbersome than non-computer based discovery because of the amount of data that may need to be collected and the persistence of such information. Information generated by computers tends to have multiple copies, versions, and can easily spread to hundreds or thousands of individuals with computers. This Electronically Stored Information (ESI) also has metadata such as creation date, modification date, file size, and sometimes who created the file or edited it. All of this information can be very useful when tying together facts but can also pose some additional challenges such as the intentional or negligent withholding, hiding, alteration or destruction of evidence. All of these factors need to be addressed when dealing with e-Discovery.

5. Identifying the Need for e-Discovery

The increase in reliance of electronic communication within businesses should strengthen the need for a document retention policy and a means of recovering archived data. A survey was recently conducted by the American Management Association and the ePolicy Institute which polled 840 businesses regarding their workplace e-mail and instant messaging policies and procedures. The survey found that "*21 percent of the businesses had had employee e-mail and IMs subpoenaed in the course of a lawsuit or regulatory investigation."* (Nelson, Olson, Simek, and ABA, 2006) Of those surveyed, thirteen percent dealt with lawsuits triggered by e-mail and only thirty-five percent actually had an e-mail retention policy. While seventy-nine percent had a written e-mail policy, only twenty percent had one for instant messaging. When discussing controls, only eleven percent had management or gateway software to monitor, purge, or retain instant message data. Despite this, "*90 percent of the respondents said they were spending as many as 90 minutes per workday on IM."* (Nelson, Olson, Simek, and ABA, 2006) Ten percent of the employees surveyed claimed to have spent at least half the workday on e-mail while the average said they spent at least a quarter of the day on it. (Nelson, Olson, Simek, and ABA, 2006) Considering these statistics were collected over five years ago, it is likely that instant messaging and e-mail usage has increased as well as the number of subpoenaed requests.

6. The Challenge

Technology makes it easier to communicate and to store valuable audit trails of business records. Unfortunately the ease of storage and the amount being stored can come back to haunt a company. Litigation is more costly and risk-filled today than ever before but not necessarily because of runaway juries or expensive trials. While these possibilities remain as real threats, "*in fact 98% of all federal cases are resolved without trial. Litigation today is difficult primarily because of discovery."* (Losey, 2008) When discussing commercial, regulatory, and employment litigation, discovery can involve forced disclosure of massive amounts of internal business records and information which can takes months to recompile. Time spent having to gather all this information can be extremely expensive when having to pay a seasoned IT professional or lawyer. "*The*

most burdensome discovery today is for email and other electronic documents located on a litigant's computers, so-called 'electronic discovery' or 'e-discovery.'" (Losey, 2008) Depending on the basis of the lawsuit and company or information being subpoenaed, it is possible for the costs involved in the e-discovery process to actually exceed the total amount in controversy. It is not just businesses that are subject to these e-discovery costs, but also state and federal government investigations as well regardless of whether or not a lawsuit was filed.

7. Forming an e-discovery Team

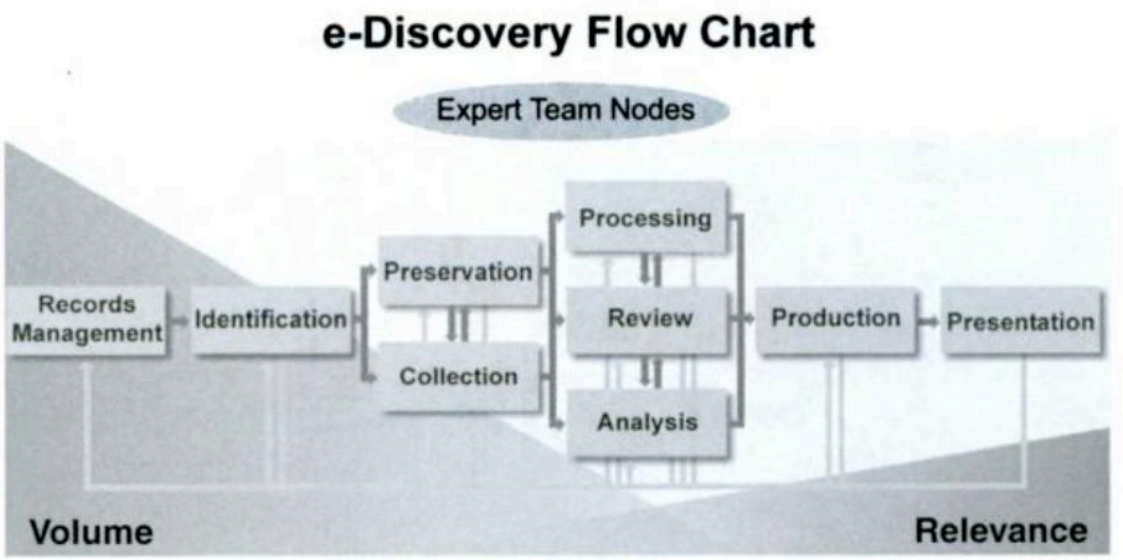
Time spent in litigation is extremely costly to any company, so it is important to resolve legal issues quickly and efficiently. Because the discovery phase of litigation has been identified as one of the most costly phases, companies should prepare for this ahead of time instead of waiting for an actual lawsuit to emerge. "*The consensus solution to this problem is the formation of an e-Discovery Team, an interdepartmental group comprised of lawyers, IT and management."* (Losey, 2008) This team of experts provide the foundation of knowledge essential to effect e-discovery which is information science, law, and technology. This multidisciplinary team approach to e-discovery has been known to work but tends to be difficult to set up because of the individual goals and motivation of each group. In order to make this team work effectively, traditional team-building techniques must be employed like establishing team goals, rewards for participation, and developing effective channels of communication. Many companies such as Cisco, Pfizer, and Merrill Lynch began developing e-discovery teams some years ago and have demonstrated "*enormous cost-savings and risk-management benefits of the internal team approach*." (Losey, 2008) Another consideration related to cost is the expense to have an IT person on the team versus another lawyer or paralegal. While it is good to have a well rounded team, consideration needs to be taken when addressing the cost per hour for each team member, depending on required skills needed to perform the work. This may also help drive the solution when determining the ease of workflow and its user interface. Will the technology solution your company is considering be easy enough for a non-technical person to manage?

8. How to Approach the Solution

The first step to taking on an e-discovery solution is to agree upon a scope and objective. Things to consider when developing the scope include budgetary constraints as well as time and resource constraints of your existing staff. It is unrealistic to assume that implementing a new technology will have little to no effect on existing IT teams and therefore should be socialized with managing directors of these areas when developing the scope. Starting out with a smaller scope, like agreeing to capture only emails, may make the most sense depending on your business model. If you are in the software industry, this may require additional discovery requirements such as hard drive images, network file share backups, and other data portability devices like thumb drives or writable DVD media. Companies of a similar size (large or small) or business model may be held to similar standards in the eyes of the court. Therefore if your company has 1000 employees and works in the financial sector, your company may be required to have the same level of controls and discovery capabilities as other companies in the same spectrum. This expectation of minimum standards is considered exercising due care when it comes to defining these requirements. This means that a judge may consider your company negligent if you do not adhere to the same minimum standards as other companies within your industry.

9. Understanding the e-discovery Process

In order to ensure the scope and objective of your solution addresses the major components of e-discovery, it will be important to understand the steps involved in the process. There are typically nine steps to the e-discovery process which are based on the industry standard "Electronic Discovery Reference Model". These are widely accepted by most e-discovery vendors and incorporate the primary functions of both the internal teams and external legal counsel. The figure below provides a high level overview of these steps.



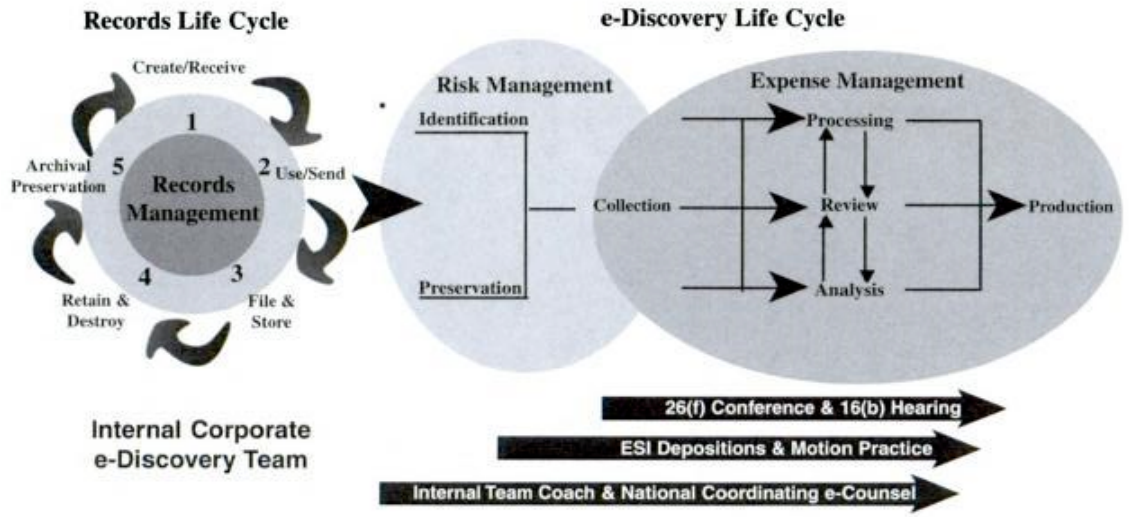
(Losey, 2008)

The e-discovery process begins with Records Management which details how data is managed and maintained throughout the e-discovery lifecycle. This phase usually begins with the establishment of an internal e-discovery preparedness and response team consisting of information security, IT, legal representatives, and key business individuals. This core team will facilitate the initial four steps of the e-discovery lifecycle as defined in the image above. The second phase is Identification which defines the scope and objective of the discovery process. This step is often initiated by a lawsuit or the anticipation of a subpoena. In this phase you will identify key witnesses, all sources of discoverable information, and its location. The third and forth steps are Preservation and Collection which detail how the data will be gathered and protected. As part of the preservation effort, companies will prepare and distribute a Litigation Hold which will require all materials related to the suit to be maintained. The hold notice will usually come from senior management and be distributed to all employees or individually potentially involved in the case. The collection process requires the team to sift through the preserved data and to maintain the relevant information for the case.

The Processing phase begins with reviewing the collected information and removing any duplicate data. Material relationships must be examined to decide if additional collection or data extraction is necessary. The Reviewing phase, which is often the most expensive, is the step where the data must be studied for relevance,

confidentiality, or redaction. This stage can take a tremendous amount of time and effort and is usually handled by a large team of attorneys. The Analysis phase is defined as the evaluation of the data to determine relevance to the case, and the identification of key issues, witnesses, and prioritizing of important documents. The final two stages are Production and Presentation which involve placing the data in a format that relates to the case. Hash marking and labeling the data are part of the Production phase. Presentation is the last stage and can be accomplished via computer screen, video, or still images. Time spent in litigation is extremely costly to any company, so it is important to resolve legal issues quickly and efficiently. The discovery phase of litigation has been identified as one of the most costly phases, as a result companies should prepare for this ahead of time instead of waiting until suit is filed.

All business records must go through a life cycle of creation, distribution or use, storing, archiving, and finally destruction. Companies should develop a record retention and destruction policy and ensure all employees abide by this policy. These documents can be used in your defense and should be relied upon to limit your e-discovery requirements. The only caveat to this defense is that these policies must be followed by all employees and be part of your business processes. The e-discovery process plugs into the records life cycle and can be broken down into a risk management phase and an expense management phase. The risk management phase addresses identification and preservation which may be part of your existing business processes. The expense management phase is enacted after a lawsuit has been filed which incorporates the collection, processing, review, analysis, and production of data. Below is a graphical example of how the records life cycle ties into the e-discovery life cycle.



(Losey, 2008)

10. Work with the legal team

After developing a firm understanding of the e-discovery life cycle, it will be important to learn the legal team's process and procedures. Identify what challenges the legal team faces and how someone from information security or a technology team could help minimize their struggles. Taking the time to document their processes from an information security perspective will also help to identify all the steps where IT could be involved to streamline the process. After documenting their processes, socialize them amongst the team and validate its accuracy and completeness. After this process has been completed, will you then be able to approach a solution that meets your customized needs.

11. Choosing the right e-discovery solution

Understanding the e-discovery life cycle will help to outline the requirements for identifying the solution that fits your company. The e-discovery team needs to decide how they will collect the data, whether over the network or to gather remotely. If many employees telecommute or travel frequently, the decision to gather discovery data remotely may be the best option. Analysis should be conducted to determine the time it takes to collect ten gigabytes of data from a user's computer. The time will vary

depending on whether the information is continuously collected over the network or gathered remotely and transmitted once the collection process has completed. A team should also consider the options of implementing a nontechnical solution which may enable a less expensive resource to perform the collection process. Along these same lines, a company should evaluate the time and money spent gathering data with a specific tool versus not having a tool in place and attempting the same collection. There is no sense in spending a fortune of money and resources to implement a specific e-discovery solution if at the end of the day the costs are equivalent to doing it manually.

11.1. Initial Steps

The first step in preparing for e-discovery is to document all your processes specific to your business. So for each phase of e-discovery (records management, identification, preservation, collection, processing, review, analysis, production, and presentation) you should identify roles, responsibilities, contact information, timelines, procedures, communication channels, and contingency plans. These processes need to be agreed upon by the e-Discovery team which may include members of legal, information technology, and management. It will be important to develop a process to track a chain of custody for the handling of artifacts and transfer between teams. This should coincide with the ability to log check-in and check-out procedures so as to keep track of who has the artifact at any given time.

11.2. Vendor Selection

After going through the exercise of documenting your processes, the e-discovery team should have a better understanding of the requirements needed for an e-discovery solution. When selecting a vendor, be sure to have a list of questions prepared ahead of time and develop a matrix to be able to compare vendor capabilities against each other. It can be a good practice to implement a weighted comparison into the matrix that assigns higher values to the more desirable qualities as opposed to the "nice to have" components. This makes it easier to distinguish between vendors and may take some of the bias out of the selection process. The evaluation process should involve all groups from the e-discovery team to ensure all aspects and concerns are addressed.

11.3. Tips when Dealing with Vendors

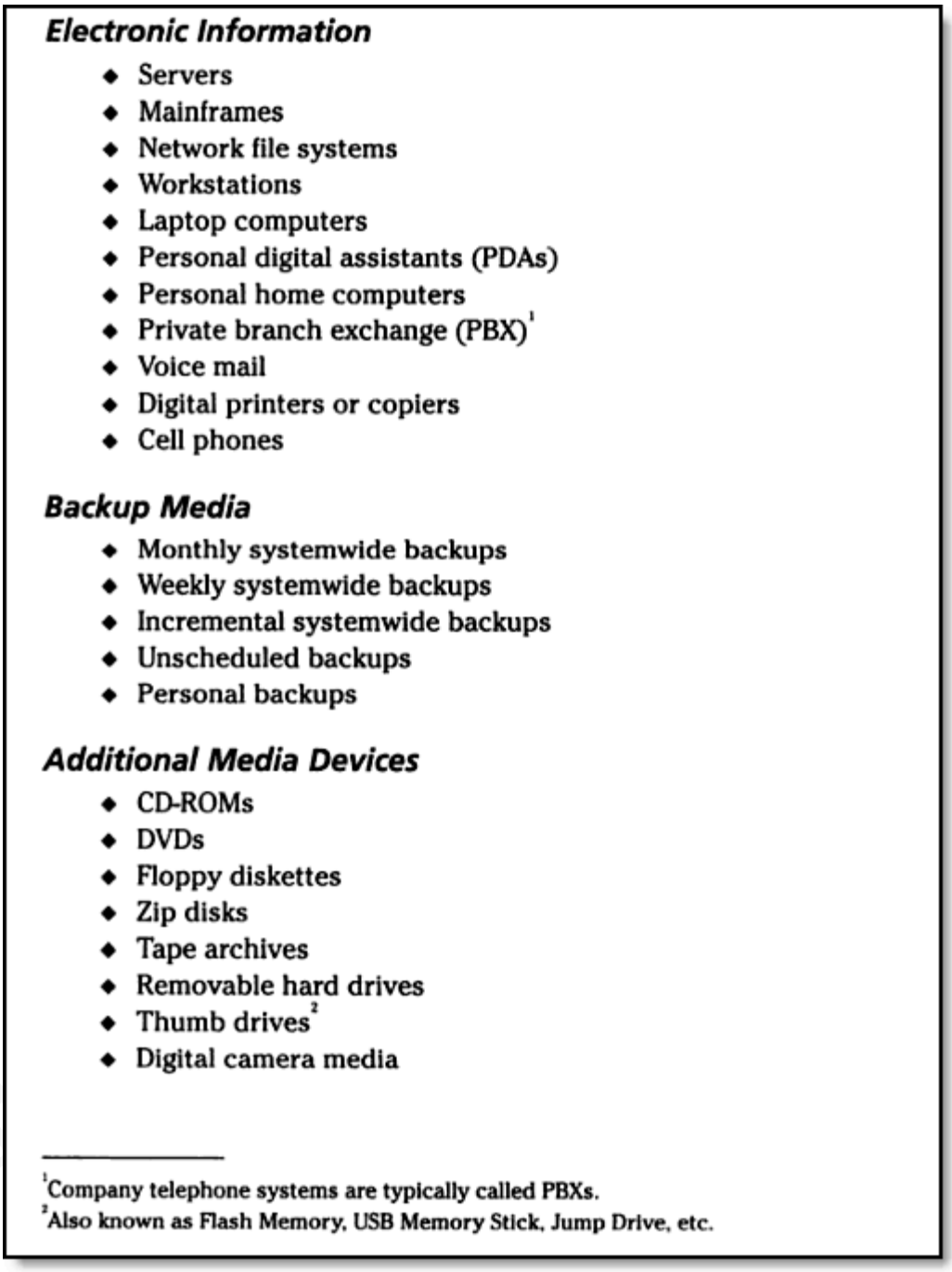
Having a good understanding of your internal processes and the requirements of e-discovery will be of great assistance in the vendor selection process. Below is a quick reference of terms that can assist when dealing with vendors.

- **Active Data:** Data on a computer that can be accessed without restoration
- **Application:** A software program such as Word or Excel
- **Attachments:** Electronic files appended to an e-mail message
- **Backup:** A copy of data for preservation purposes; data is often backed-up on a network file server or backup tapes
- **Burn:** Computer slang for "copy" (i.e. to burn files to a CD)
- **CD-ROM:** A common data storage medium, often used to carry, trade and produce electronic files
- **Custodian:** Person having control of an electronic file; often referred to as the "employee source" during the discovery process
- **Data:** Electronic information stored on a computer
- **De-Duplication:** The process of removing duplicate files from a document population
- **Deleted File:** A file with disk space that has been designated as available for reuse; the deleted file remains intact until it is overwritten
- **E-mail:** Electronic mail or computer-based mail
- **E-mail String:** A series of e-mails linked together by e-mail responses or "forwards"
- **Electronic Discovery:** The process of collecting (also called "harvesting"), preparing, reviewing, and producing electronic documents in the context of the legal process
- **Electronic Image:** An electronic or digital picture of a document; the most common image used in E-Discovery is TIFF (Tagged Information File Format)
- **File:** Data stored under a specific name
- **File Format:** The organization or characteristics of a file that allow it to be used with certain software programs
- **File Server:** A computer designated to serve as the main storage location for other computers on a network
- **Floppy Disc:** A common storage medium used to copy and port relatively small amounts of data
- **Hard Drive:** A computer's primary data storage device
- **Harvesting:** The process of retrieving or collecting electronic data from storage media or devices; an E-Discovery vendor "harvests" electronic data from computer hard drives, file servers, CDs, and backup tapes for processing and load to storage media or a database management system
- **Keyword Search:** A search – of the text of documents in a database – designed to retrieve documents containing a "keyword;" generally the most basic of a number of searches; depending on the software application's capabilities, a variety of advanced searches can be performed

- **Meta data:** Data about data; resides in the shadows of a document and usually includes information such as, author, recipient, creation date, modified date, etc.
- **Native File:** A file in its original file format that has not been converted to a digital image or other file format
- **Network:** A group of computers linked together ("networked") for the exchange and sharing of data
- **OCR Text:** Optical Character Recognition; searchable text that corresponds to a document image; an OCR software program designed to "read" a document image generates OCR text.
- **PC:** Personal computer

(Yacano, 2004)

Having a list of media that you may be responsible for preserving or discovering will also be helpful when speaking with vendors to determine their capabilities. Below is a list of standard media types that may be in use with your company.



Electronic Information

- Servers
- Mainframes
- Network file systems
- Workstations
- Laptop computers
- Personal digital assistants (PDAs)
- Personal home computers
- Private branch exchange (PBX)[1]
- Voice mail
- Digital printers or copiers
- Cell phones

Backup Media

- Monthly systemwide backups
- Weekly systemwide backups
- Incremental systemwide backups
- Unscheduled backups
- Personal backups

Additional Media Devices

- CD-ROMs
- DVDs
- Floppy diskettes
- Zip disks
- Tape archives
- Removable hard drives
- Thumb drives[2]
- Digital camera media

[1]Company telephone systems are typically called PBXs.
[2]Also known as Flash Memory, USB Memory Stick, Jump Drive, etc.

(Nelson, Olson, Simek, and ABA, 2006)

11.4. Tips for Vetting the Vendors

Knowing the e-discovery process inside and out is obviously helpful but if you cannot be an "e-discovery guru" yourself, be sure you have someone on your team that can be a subject matter expert in this area. Staying ahead of the curve or knowing more than you have to can always be helpful because it may avoid having to make uneducated last-minute decisions. Another key component is to meet with the vendors and establish a relationship with them so as to learn their product capabilities and pricing before it comes down to "crunch time". If possible, take the time to visit the vendors at their location to see their support structure and whether they sub-contract all or most of their services. This may also provide the opportunity to meet with more of the technical staff to get a better understanding of the product as opposed to the sales staff. Ensure to always check references to gather an idea of product and support satisfaction levels of other companies of a similar size or business model. (Yacano, 2004)

12. Documenting an e-Discovery Handbook

After the final processes and vendor solutions have been laid out, you should consider capturing this information in an e-discovery handbook. In this handbook, which can be brief and high-level, you can specify what your company is responsible for doing when it comes to e-discovery:

- Data your company considers discoverable: file types and where they sit, vectors of transmission (IM, email, phone messages, etc.)
- The location of this data
- The data **not** considered discoverable, where it will not look, and the reason for the limitation (usually accessibility)
- Document-retention policy
- High-level process for the lifecycle of a case, from notification to completion.

13. Conclusion

The interaction between Information Security and Legal teams can be an unpleasant experience if the proper time is not dedicated prior to litigation to learn each other's objectives, roles, and responsibilities. Having an understanding of the current business processes, technical capabilities, and legal requirements involved with e-discovery will help to ensure both parties are working toward a common objective. The development of an e-discovery team comprised of IT, legal, and management has been proven effective in helping to enhance communication and interdepartmental process understanding. Working together the e-discovery team can document current processes and begin to effectively evaluate a solution that will assist in the e-discovery life cycle. The goal of the team will be to identify a solution that fits their business model and to reduce the overall risk (financial or legal) associated with e-discovery.

14. References

Cummings, Joanne (2007, May 21). Sloppy e-discovery can cost you millions. Retrieved July 31, 2009, from Network World Web site: http://www.networkworld.com/supp/2007/ndc3/052107-ediscovery-readiness.html

Gupta, Jatinder N. D., & Sharma, Sushil K. (2008), *Handbook of Research on Information Security and Assurance*. Hershey, PA: IGI Publishing.

Krause, Micki, & Tipton, Harold F (2006). *Information Security Management Handbook*. Danvers, MA: CRC Press.

Losey, Ralph C. (2008). *e-Discovery*. Chicago, IL: American Bar Association Publishing

Nelson, Sharon D., Olson, Bruce A., Simek, John W., & American Bar Association. Section of Law Practice Management, (2006). *The Electronic Evidence and Discovery Handbook*. Chicago, IL: American Bar Association Publishing.

Yacano, Mark (2004, July). Vetting Your E-Discovery Vendor: The Lawyer's Perspective. Retrieved June 17, 2009, from Law Practice Today Web site: http://www.abanet.org/lpm/lpt/articles/ftr07043.html

Last Updated: July 25th, 2017

Upcoming Training

SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
Data Breach Summit & Training	**Chicago, IL**	**Sep 25, 2017 - Oct 02, 2017**	**Live Event**
SANS vLive - LEG523: Law of Data Security and Investigations	**LEG523 - 201710,**	**Oct 09, 2017 - Nov 08, 2017**	**vLive**
SANS Dallas 2018	**Dallas, TX**	**Feb 19, 2018 - Feb 24, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**