Interested in learning more about security?

SANS Institute InfoSec Reading Room

What Companies need to consider for e-Discovery

Within the legal environment, Discovery is the process of identifying, locating, preserving, securing, collecting, preparing, reviewing, and producing facts, information, and materials for the purpose of producing/obtaining evidence for utilization in the legal process. Electronic Discovery (e-Discovery) is an extension of these processes into the digital environment and Electronically Stored Information (ESI). Legal departments are ill-prepared to deal with the digital environment of a business. Increasingly they are ...

What Companies need to consider for e-Discovery

How Information Security Can Help the Organization Succeed

GIAC (GLSC) Gold Certification

GIAC ID#

Author: Thomas Vines, GIAC.Thomas.Vines@gmail.com

Advisor: Christopher Walker, CISSP

Accepted: August 20, 2015

Abstract

Within the legal environment, Discovery is the process of identifying, locating, preserving, securing, collecting, preparing, reviewing, and producing facts, information, and materials for the purpose of producing/obtaining evidence for utilization in the legal process. Electronic Discovery (e-Discovery) is an extension of these processes into the digital environment and Electronically Stored Information (ESI). Legal departments are ill-prepared to deal with the digital environment of a business. Increasingly they are turning to the company's Information Technology (IT) department in order to identify, locate, preserve, and collect ESI. This is not break/fix work that is typical in IT operations. This is a new area of Data Governance and Records Information Management. This paper explores the relationships between Executive Management, Legal, Risk Management, IT, and Security in fulfilling the demands and obligations for defensible e-Discovery. This analysis includes a discussion of the Electronic Discovery Reference Model (ERDM) and its integration with Information Governance Reference Model (IGRM).

1.0 Introduction

In a civil lawsuit, first the pleadings are filed with the court system. Within the pleadings, the parties define their dispute by outlining their claims and defenses against these claims. The pleadings typically contain complaint or petition, answer, counterclaim and other proceedings. These are not intended to be exhaustive compendiums of all of the claims, defenses, and evidence that will be presented in the case. The Pleadings contain notifications to the opposing party or parties of what each side believes will be the issues involved, and what positions they will take (American Bar Association, 2015).

The second stage is discovery. During this phase, the parties use devices such as document requests, interrogatories, and depositions, to flesh out and support the claims and defenses set forth in the pleadings. Electronic Discovery ("e-Discovery") and Discovery are legal ideals that support free and transparent litigation with the United States. Both standards require the other party, plaintiff, or defendant, to share evidence. The formal definition from the Sedona Conference makes clear the distinct processes within e-Discovery declaring that, "Electronic Discovery is the process of identifying, preserving, collecting, preparing, analyzing, reviewing, and producing Electronically Stored Information ("ESI") relevant to pending or anticipated litigation, or requested in government inquiries. E-Discovery includes gathering ESI from numerous sources, reviewing and analyzing its relevance and the applicability of any privileges or protections from disclosure, and then producing it to an outside party." (The Sedona Conference, 2013). In the US Federal system, three primary rules govern and define these processes in Federal Rules of Civil Procedure. The rules are (1) Rule 26(a) Discovery and the Duty to Disclose, (2) Rule 34(a) Producing documents and ESI, and (3) Rule 45(a) Subpoena. The e-Discovery tasks include a process of identifying, collecting, and preserving ESI relating to or originating from a custodian (e.g. the person being sued). The relevant ESI pertaining to the litigation is then processed, reviewed, and produced as evidence (EDRM.NET, 2014).

Rule 26(a) of the Federal Rules of Civil Procedure allows for the discovery or sharing of "documents, electronically stored information, and tangible things" in the responding party's "possession, custody, or control" (Cornell University Law School, 2005). Similarly, Rule 34(a) and Rule 45(a) obligate a party responding to a document request or subpoena to produce "documents, electronically stored information, and tangible things" in that party's "possession, custody, or control" (The Sedona Conference, 2015).

However, “control” has not been defined in the Federal Rules, and the Federal case law results are a chaotic morass of binding and non-binding findings and opinions (The Sedona Conference, 2015).

2.0 Expectations of Control

Generally, the US Federal courts agree that “Control does not require legal ownership or actual physical possession of documents at issue; rather ‘documents are considered to be under a party's control when that party has the right, authority, or practical ability to obtain the documents from a non-party to the action’” (*Grayson v. Cathcart* , 2013). This duty [to preserve] requires the party to “identify, locate, and maintain information that is relevant to specific, predictable, and identifiable litigation” and to “notify the opposing party of evidence in the hands of third parties” (*Silvestri v. General Motors*, 2001).

Case Law, which are legal principles applied in judicial decisions (Law.com, 2015), suggest that corporations have several factors to manage that directly affect business operations. The courts have an expectation that companies know they may be litigates and should anticipate lawsuits. At the time of anticipated legal action, companies should retain all of the data relevant to the legal action. This legal expectation extends to both the company and the individuals involved in the litigation. Pertinent evidence may be in corporate user drives, corporate email systems, and numerous other places. Likewise, they may not be on company infrastructure but on litigant-owned personal smartphones, laptops, and in cloud storage. Companies need to have a governance structure, whereby they know where ESI is saved, how it was saved, who had access to it, who in fact saved it, and what it contains. These indirect requirements create a legal environment where records management and information governance becomes a business necessity to defend against litigation.

The issue of control of documents becomes very complex as workforce members (Healthcare Information and Management Systems, 2014) store information on a variety of digital assets. They may include the traditional company controlled IT assets like desktops, laptops, as well as untraditional storage locals like company issued smartphones, tablets, cloud storage. Another variety of devices to be concerned with are personally owned digital assets. For every corporate controlled digital asset, the consumerization of information technology has enabled workforce members to operate their own Data Center full of technology. An ever-increasing percentage of the knowledge workforce is inadvertently blurring the boundaries between the corporate information they work with every day to their own personal technology and information. The membrane between corporate technology and personal

technology has become very permeable. In a digital world, storing zero or ones is practically universal, storing a document on a USB drive, or on a SD card, or a smart phone or a tablet and moving that document to and from corporate IT environments is trivial in most business settings. Employees, often with the motivation to increase their personal productivity, store data on personally owned and controlled technology assets. In many corporate environments, this data migration goes on undetected. The move to productivity can be a strategic economic play for businesses to minimize costs while boosting efficiency. Allowing the workforce to use their own digital assets can to lessen the economic impact of outfitting a workforce with the latest and greatest technology (György, Cleven, Uebernickel, & Brenner, 2012). Instead, companies issue a stipend to the workforce member to acquire their own technology, thus reducing administrative overhead of provisioning and procurement of technology. Regardless of the technology controls and administration controls, or lack thereof, Custodians and Corporations have a legal expectation to produce any and all relevant data during e-Discovery (Murphy, 2011) .

Self-managed digital assists have given rise to Shadow IT (SIT) (György, Cleven, Uebernickel, & Brenner, 2012). SIT is often the unorthodox use of IT without the corporate direction, control, staffing, or planning of traditional Information Technology management (Gallagher, 2015). The phenomenon of personally owned self-sufficient digital knowledge workers has fueled the growth of SIT. The continued consumerism of IT that has also lead to an ever-increasing capability of SIT. SIT is often a user-driven response to the rigid bureaucratic style of some IT organizations (Myers, 2015). This more organic and often unmanaged technology of bring your own device (BYOD) environments may help the immediate need of a company to minimize workforce on-boarding, but fuels the negative business impacts (György, Cleven, Uebernickel, & Brenner, 2012) of vulnerability, non-compliance and litigation. SIT continues to be under the control of the Corporation. The Courts do not make any distinction between user-driven SIT and fully managed corporate IT. This may create a situation where unknown data in an unknown SIT system is missed. That missed data could lead to claims of bad faith and spoliation (Kroll OnTrack, 2013). Custodians and Corporations, along with the Attorneys representing them, have a duty to uncover SIT systems and produce relevant data. (Reginald W. Jackson, 2012).

An often cited example of the vastness of data and the undue burden corporations bear of sorting and reviewing states (The Sedona Conference, 2015), "one gigabyte of electronic information can generate approximately 70,000 to 80,000 pages of text, or 35 to 40 banker's boxes of documents (at 2,000 pages

per box). Thus, a 250 gigabyte storage device (e.g., a laptop or hard drive), theoretically, could hold as much as the equivalent of 8,750 to 10,000 banker's boxes of documents. Even if only 10% of a computer's available capacity today contains user-created information (as distinguished from application programs, operating systems, utilities, etc.), attorneys still would need to consider and potentially review 1,750,000 to 2,000,000 pages per device." (William W. Belt, 2012)

The problems with e-Discovery that this example contains are important items to consider. Finding the data that a custodian stored somewhere in the environment is a big problem. Each Megabyte of data may be important. Collecting a copy of that data is a big problem. Storing a copy of that data is a big problem. Processing all that data into an easily searchable form is a big problem. Getting an attorney to review all that data is a very expensive problem. Producing all that data to a receiving party in litigation or the courts is a problem. Lawsuits and the conditions they create if left unmanaged, uncontrolled, and unplanned for can kill businesses from startups (Sullivan, 2015), to well established companies (Bort, 2015), and sometimes entire industries (Wyatt, 2015).

2.1 Custodian Identification

In a large corporation, with significant employment base, custodian identification can be difficult. The difficulty of custodian identification is shared on both sides of the litigation. The identification of the Custodians can be confusing. The plaintiff may identify a person involved with a case as Jim Smith[1], but whose real name is David James Smith Jr. All the while, David James Smith Sr. also works at the corporation but was in no way involved with the litigation. Other members of the workforce like contractors, vendors, and volunteers may also be parties to the litigation and their identification can be just as problematic for both plaintiff and defense. Corporations are obligated as a Records Owner (The Sedona Conference Glossary, 2014) and commonly considered a party to the litigation. Just as individuals can be identified as custodians that work for a corporation, the corporation itself can be a litigant. Corporations are indeed people too (Totenberg, 2014). The interview of key players involved with the litigation is one practical tool for sorting out who is who. The value of the interviews can define e-Discovery's efforts and proportionality. Interview findings have a direct impact upon e-Discovery agreement that the two opposing counsels are required to create.

[1] Totally fictional example, no Jim Smiths were sued or harmed in anyway in crafting this paper.

Once custodians have been agreed upon by the attorneys, their data relevant to the case needs to be Identified, Collection, and Preserved (ICP) in relation to the entire e-Discovery Reference Model Pictured following in Figure 1. (EDRM.NET, 2014)

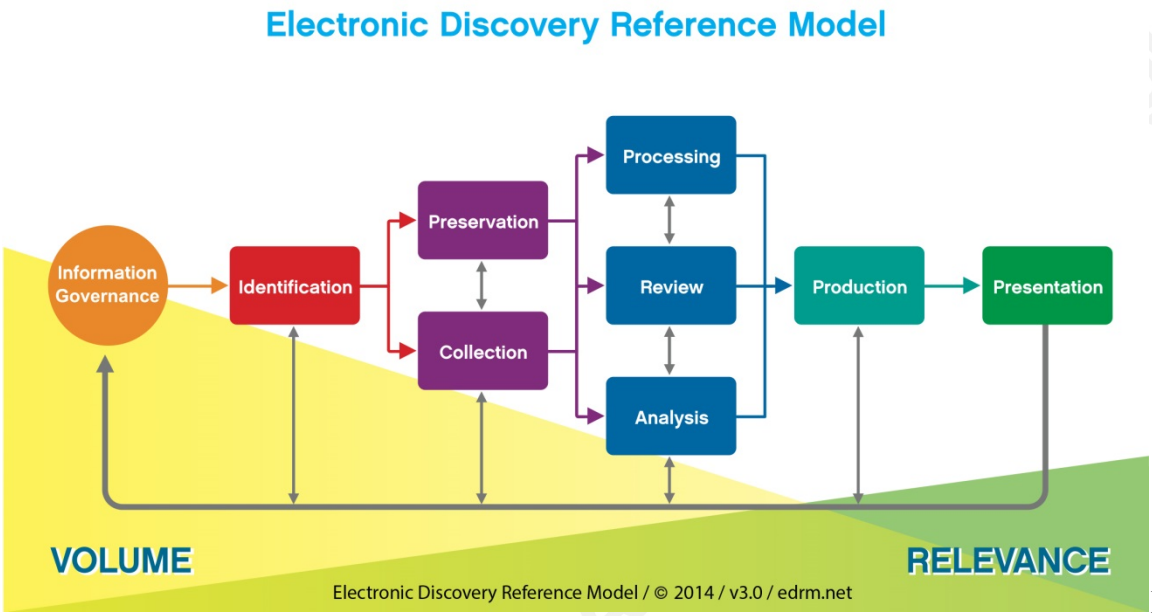

Figure 1.

Corporations are obligated to conduct an extensive search of their systems in order to ensure that all relevant data is presented to the Courts (The Sedona Conference, 2015). Determining where the relevant corporate ESI is stored can be an enormous undertaking. Likewise, Custodian ESI is often times stored onto the entities' technology environment, as well as a variety of smartphones, tablets, home PCs, and in the cloud. Typical user created information includes documents, email, database, and other information assets. Information assets under the control of the user can be stored anywhere the user has the authorization to write information. If custodial data is spread across a known work desktop, but also on an unknown home laptop, an unknown tablet, and an unknown smartphone the self-evident problem of data volume and variety becomes clear (Boudreau, 2010). It enables velocity of business and its perceived need for productivity; however, it creates a situation where the unknown and unmanaged data repositories contain the majority of potentially relevant data that the company has a duty to preserve. Each company is expected to produce relevant evidence, even though their IT/SIT has a lack of IT management, vendor oversight, or managerial governance (*Logtale, Ltd. v. IKOR, Inc.*, 2013).

2.2 Data Map

Each of the Custodian's digital assets creates a reference point to map out where potentially relevant data may be located. These different points create the data map (Schuler, 2009) that can be used to locate and identify the data to be preserved as evidence. The data map is directly tied to the custodian's use of digital assets both corporate controlled and personally owned. The custodian has created data, such as, documents, email, text messages, and "any other tangle thing" relevant to the matter need to be collected and preserved. This is usually where IT is recruited by Legal to assist with the data gathering. Information Technologies (IT) processes and procedures are leveraged not for break fix or operational concerns, but to comprehensively identify and locate the data created, used, and stored.

Within most IT organizations, there is a lack of awareness when it comes to unstructured user created information stored on servers, PC, NAS, and SAN infrastructure. Server engineers focus on the optimization of services and not the orderly storage of documents. Application developers do not value the storage of ESI either. Not even the Storage Engineers dive deep into the morass of managing unstructured data. In the majority of enterprises operating on premise Microsoft infrastructure; the provisioning of accounts, the shares they may access and store data, as well as the determination of who owns shares is a nether world of ghosts and apparitions (Toshniwal, 2015). Leading researchers in 2010, a mere five years ago, estimated that 13 Exabyte were created by users in enterprises (Computer Research Association, 2012). As early as 2011, Gartner Research described this as big data's velocity, variety, variability and volume factors that each enterprise must manage (Gartner Group, 2011).

Most businesses are focused on just three things, numbers, numbers, and numbers. Profit numbers, sales numbers, key performance indicators, balance scorecards and other meta-business quantification integers. Within companies, decisions to manage unstructured user created data and apply business value taxonomy to it are often neglected. Many companies do not have business record retention schedules or records management (International Organization for Standardization - ISO, 2001). Along with records management itself, companies often neglect the need for staffing, see the value in Records Information Management, and fail to perform a cost benefit analysis to establish the bases for cost justification. Companies have profit motivations first and foremost. They are organized to perform revenue-generating activities. They are not constructed with litigation defense in mind (Murphy, 2011).

The neglect is reversed when litigation shocks the company. The negative business impacts from a lost lawsuit, even if settled, can be very great. The scramble to defend, the frantic search for ESI, the wasted labor, and the loss of productivity can be enormous. This urgent work takes place at the expense of the company's profit engine and furthers the dramatic negative business impact. This condition is exacerbated if additional losses from litigation occurs. In the United States Federal Court System, the Federal Rules of Civil Procedure (FRCP), which was amended in December 2006 to address e-Discovery, sets out several timelines and may give as little as 30 days from initial legal meetings to start producing relevant data (e-Discovery HQ, 2012).

Companies would be wise to prevent the mad scramble for ESI. Benjamin Franklin's axiom that "an ounce of prevention is worth a pound of cure" is as true today as it was when Franklin made the quote on February 4, 1735 issue of The Pennsylvania Gazette. The scramble to defend, the frantic search for ESI, the wasted labor, and the loss of productivity can be eliminated by executive management designating a cross-disciplined group of experts who are empowered to meet the challenges of e-Discovery response.

3.0 The Need for Records Management

The ISO 15489-1: 2001 standard ("ISO 15489-1:2001") defines records management as "[the] field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including the processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records". Records Information Management (RIM) is a critical need for the companies' response to litigation so that it functions effectively. Whenever the company is notified of litigation or when the company can reasonably discern that they are about to be sued, the company should halt the normal disposition of records that may be relevant to the litigation (Schuler, 2009). Therefore knowing what records surround the litigation event is critical. Knowing in advance, who is involved, the hardware they have issued, the software they have installed, the mobile device they use, the emails accounts they use, and the relevant records stored upon each device gives new meaning to custodial big data. Each custodian must be examined for the volume of data per digital asset, variety of business records, variability of file formats and storage locations, and lastly the velocity at which they can be preserved as potential evidence.

The most fundamental task of determining which file is relevant to litigation within a companywide public network share becomes monumental. Depending on the operating system and software, their versions, and other application specific settings, there may be metadata concerning the author, creation date, or other elements to attribute the material to an individual custodian in a reliable manner. However, metadata artifacts do not exist or present themselves reliability in all files. Other files saved to the Custodians' personal network share, their business computer, smartphone, or tablet are presumed to be of their own creation, but there is little in forensic determinations that can be definitive.

This technical limitation is just one reason to engage with the Custodians directly to ask where they saved ESI. Where material associated with the litigation incident may be stored, and if material is outside of the corporations' technical environment. This may include personal cloud storage, non-corporate computer assets like a home PC, or a personal smart phone. Custodians generally understand that corporate email is subject to hold, but other potential evidence like voice mail may be just as important (Aversano, 2015). These interviews are crucial to developing the data map. The interviews themselves may become evidence of the attorney's comprehensiveness, corporations due diligence. Interviews can also be used to create custodian awareness of the custodian's duty to preserve culpability.

Another factor supporting the need for Records Information Management is the often-lauded 30(b)(6) witness. This person is the corporation's designate who responds to e-Discovery dispositions where receiving counsel may interrogate. During the deposition, the opposing counsel may test the witness to ensure that a comprehensive e-Discovery program is being well managed. Selecting, staffing and training a 30(b)(6) witness prepares the organization for success (Young, 2011). However, incorrect or incompetent e-Discovery program efforts have, for more than a decade, been grounds for legal relief *(AdvantaCare Health Partners, LP v. AccessIV*, 2004). Getting records management to operate effectively requires the whole organization to be engaged.

Records Management is integral to the disposition of data. This function leads not only the value definition of data, but also what happens to the data when it is no longer needed by the business. Companies routinely auto-delete email, documents and other data in an effort to control the disk space usage and ensure tidiness of the data storage environment *(Apple Inc. v. Samsung Electronics Co. Ltd et al,* 2012). Enforcing retention schedules to delete irrelevant data saves disk space and controls costs of operations. Equally, when a workforce member leaves the employer and they are not under legal hold, the disposition of their data on company controlled digital assets is important. RIM functions typically

address the litigation hold in auto-delete environments. Both unmanaged and over aggressive auto-delete environments can generate claims of spoliation (*Mosaid v. Samsung*, 2004). Defensible strategies for auto-delete and other forms of disposition must be considered and reviewed as the changing legal landscape shifts (Aversano, 2015).

4.0 Information Governance Team

Within the United States and its overly litigious environment, being prepared to defend against lawsuits in a vigorously manner is a key legal strategy (Schuler, 2009). Records management is the planning, controlling, directing, organizing, training, promoting and other managerial activities involving the life-cycle of information, including creation, maintenance (use, storage, retrieval) and disposition, regardless of media (The Sedona Conference Glossary, 2014). Within the e-Discovery processes, the timely identification of those involved and relevant to the case, what data they created, and where that data is stored that pertains to the lawsuit is crucial to fulfilling the courts expectations.

This is where Information Governance enables more economic, comprehensive, and efficient e-Discovery. Information governance is the comprehensive, inter-disciplinary framework of policies, procedures, and controls used by mature organizations to maximize the value of an organization's information while minimizing associated risks by incorporating the requirements of: (1) e-Discovery, (2) records & information management, and (3) privacy/security into the process of making decisions about information (The Sedona Conference, 2013). Within the unified governance of the Information Governance Reference Model (IGRM), collaboration between Legal, Risk Management, IT, Privacy, Security, and the Business provide the bases for the value of information (EDRM.NET, 2012). The value of information, the legal duty to preserve, the obligation to secure and safeguard, and ultimately the decision to dispose of data is dependent on knowing who created the data, for what purpose, the current and future need for the data, and the cost to retain and archive. Said another way, the direct value of unstructured data is directly proportional to how the data is used, its classification, and governance controls in place.

Most Information Security teams are familiar with data classification. The schedule of Private, Public, Confidential, and Restricted data classifications stretches back beyond the 1930's (U.S. Army, 1936). Likewise, processes concerning Legal, Regulations, Investigations, and Compliance issues are commonly considered a key subcomponent of the Information Security Program (ISC², 1992). The

Information Security department typically has a pre-established working relationships with Legal, and is well positioned to assist Legal as part of the litigation support function. Insider threats, incident handling, and lost or stolen equipment incidents trigger a certain degree of understanding concerning the legal environment along with technical and forensic methods used to defend the enterprise. Information Security (IS) is one of the few IT departments that routinely maps data in order to protect and safeguard the most valuable data. This data centric form of risk mitigation in a defense-in-depth strategy is well defined. The Information Security department is uniquely qualified due to the protection of high value data to extend the definition from trade secrets, intellectual property as well as customer data like Personally Identifiable Information (PII) and electronic Protected Healthcare Information (ePHI) to include Records, ESI, and other custodian data stored on various digital assets.

Knowing what hardware is on the network and what software is on that hardware are among the most critical security controls for an effective security program (SANS CSC, 2015). Linking this data set to individuals that use the hardware can be a challenging task. However, several tools can help identify what users have logged on to which PC, Laptop, or Server. One tool is Microsoft's SCCM (System Center Configuration Manager). Within its many reports are detailed login information that includes user and workstation. PowerShell is another powerful tool that can support the efforts to gather data. PowerShell scripts can interrogate Active Directory and any of its objects like business computers. It has the flexibility to gather data and take actions to support the collections of user created data.

Analyzing user permissions is another specialty of Information Security. Where a user can, store information and where they did store information are two very different questions. Mapping out a particular user's network drives can also be a challenge. Assessing the Microsoft Global Policy Objects (GPO's), Login Scripts and other methods that automatically connect network drives is one part of the equation. Other variables include if the user mapped drives of their own accord on the particular workstations they use.

5.0 e-Discovery Incident Response Team (eDIRT)

Generally, the eDIRT needs a cross-disciplined group of experts that are empowered to meet the challenges of e-Discovery responses that directly corresponds to the needs of the specific litigation. Companies should structure their e-Discovery incident response team (eDIRT) to respond to the different facets of the case. Each case may be different and require different groups and stakeholders

(The Sedona Conference, 2013). Similar to disaster recovery processes, the appropriate collaboration and consensus building between business leaders, legal attorneys and staff, HR leaders, IT and IS must take place to effectively deal with the legal matter (Schuler, 2009).

Collaboration with Information Security can play a key role due to its experience in incident handling. The litigation event is another type of incident that needs handling. Similarly, e-Discovery is just another incident type that needs to be managed. This line of reasoning takes incident handling from a security incident or a malware incident into a proposed legal incident handling process based on information security practices. Information security practices concerning incident-handling primary revolve around two major frameworks, the Information Technology Infrastructure Library (ITIL) and the National Institute of Standards and Technology (NIST) Computer Security Incident Handling Guide SP 800-61. ITIL separates incident management into six basic components; incident detection and recording, classification and initial support, investigation and diagnosis, resolution and recovery, incident closure, and finally communications (ITIL, 2011). NIST Special Publication 800-61 Revision 2 outlines the process as preparation, detection and analysis, containment, eradication and recovery, followed by lessons learned (NIST, 2012). A litigation event is a trigger to assemble a team of cross-domain experts to resolve the incident. This is analogous to the tradition malware incident that information security performs in conjunction with other parts of IT and the Business. The litigation event fits in nicely to this well documented process flow. The Early Case Assessment (ECA) is analogous to the investigation and diagnosis of the ITIL process, while meshing into to the analysis and containment process steps of the NIST 800-61 Revision 2 practice. Other incident handling processes are easily adapted to support the Litigation incident paradigm.

The eDIRT can have many participants, but the core of the team is the managing attorney, e-Discovery coordinators, predetermined 30(b)(6) witness, and the litigation support team. In certain cases, the attorneys may bring in HR, corporate communications, or any number of stakeholders to sort through the claims. The eDIRT has to be lead and managed by an attorney (Schuler, 2009). E-Discovery is a legal sub-process and requires attorneys to guide and manage each aspect of litigation. Attorneys have a duty of supervision when it comes to e-Discovery to ensure the work is being done accurately (Association of Certified e-Disocvery Specialists, 2014). Additionally, attorneys have a duty to ensure that the e-Discovery efforts are with the bounds of the law. This obligation creates a duty for the

attorney responsible for leading the eDIRT to understand how the ESI is identified, collected, and preserved by the staff assisting the attorney with the case.

Generally, the e-Discovery coordinators working for the legal department are responsible for organizing each party's e-Discovery efforts. This is to insure consistency and thoroughness to facilitate the e-Discovery process (Ohio Northern District Federal Courts, 2011). Within the Federal Rules of Civil Procedure (FRCP) at rule 30(b)(6), it allows for a corporate entity to provide a person or group of individuals that are qualified to answer the questions on behalf of the corporation. Because of the duty under Rule 30(b)(6) that the witness "must testify about information known or reasonably available to the organization," (Young, 2011) the witness must be familiar with the subject to be covered in the deposition. In addition, the witness must be fully aware that the testimony is that of the organization and not for them personally and be able to differentiate between the two.

Litigation Support (Lit-Support) is where the bulk of e-Discovery tasks are performed. Within the Legal department, this may include paralegals, investigators, and other staff. It also includes the data analysis and IT work necessary to build the data map, identifying where the data is located, collecting the data, and preservation the data. IT and Legal must work together to identify, collect, and preserve the relevant ESI. Factors that can increase the effort include size of enterprise, size of storage environment, local workstation storage, removal media, smart phones, shared drives, email environments, and document management environments just to name a few. Each of these data map locations will need to be vetted with the managing attorney. This may confuse the normal IT management hierarchy. Management needs to plan for this eventuality. Within the cases activities, the managing attorney must direct the Lit-Support team. This could create a situation where traditional IT tasks are deprioritized until the legal matter work is complete. Equally, this may cause problems if a security incident occurs at the same time a legal matter is occurring. Staffing for these conflicts and anticipating problems like these will help form the necessary organizing and controlling procedures necessary to ensure success.

6.0 Defensible Data Collections

If the requesting parties to the case have reasonable doubts about the producing party's production of evidence, they may move to perform discovery about the e-Discovery processes, its management, and methods. The most common form is the deposition under the FRCP 30(b)(6). Another avenue would be

to make a spoliation claim. Courts have agreed that, "Spoliation is the destruction or significant alteration of evidence, or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation." (*West v. Goodyear Tire & Rubber Co.*, 1999). Bad acts in the e-Discovery process can be very serious for the attorneys leading the legal matter (Kroll OnTrack, 2013). The courts in such cases like *Zubulake v. UBS Warburg* and *Coleman v. Morgan Stanley* have sent a strong message to attorneys and their staff that failure to meet the due diligence and responsiveness requirements can be career ending (Schuler, 2009).

An attorney cross-examining a 30(b)(6) witness, as all cross-examining attorneys do, will try to show that the witness, and the corporate entity they represent, acted in bad faith. Bad faith includes, but is not limited to, acts such as hiding or destroying documents, misleading interpretations of company practices, or anything that may show that documents slipped through the cracks of e-Discovery (Reginald W. Jackson, 2012). Another objective is to tease out previously hidden or camouflaged positions on issues that they have avoided in written interrogatories (Jackson, 2011). When combined these two objectives place the evidence collected from the witness in a dangerous light under intense scrutiny. The 30(b)(6) witness deposition can increase or decrease an e-Discovery dispute that may end up in spoliation claims and other contested ESI and e-Discovery issues. The 30(b)(6) witness is a prepared company's Swiss army knife, able to save and settle disputes before they become e-Discovery issues. Ill-prepared companies that place an unprepared or unknowledgeable witness in this role face significant danger (*Resolution Trust Corporation Fa v. Southern Union Company Inc.*, 1993).

7.0 What Companies Need to Consider

Prepare for litigation. Within each concept touched on by this paper, the recurring theme of preparation stands out. Executive management must lead the Planning, Organizing, Staffing, Directing, and Controlling of the enterprise (Koontz, 1955). Executive management must understand the value of records management, as well as how the businesses revenue generating machinery creates, uses, and stores data. This knowledge is the fulcrum used to move the company from an exposed position of danger to a prepared concern. Before litigation occurs, executive management at medium and large firms must plan and organize for litigation. Organizing an information governance program to manage the data, measure its value, and enforce retention periods is a basic enabler. Establishing control mechanisms to identify where data is stored, and by whom, and for what purposes is only something

executive management can direct is another basic enabler. Executive management must make the decision to enable an economic response to e-Discovery, or deal with the aftermath of being ill-prepared.

Establishing and staffing an Information Governance Team/Records Information Management (IGT/RIM) functions is expensive. For some smaller companies it may be impossible to fund and staff adequately. Often these are the same types of businesses that are destroyed by litigation (Bort, 2015). The rigor required in establishing data classification taxonomies and ownership of user created content is a vast challenge. Managing the digital identities and privileges to create and store user created content is one issue that must be addressed. Another is the user driven innovation and SIT. Lastly, to operate a functional IGT/RIM function the organization must recognize a return on its investment (ROI). The ROI must be an integral part of the IGT/RIM methodology. It must be managed effectively, and reported upon to executive management.

Establishing a team to respond to the threats of litigation takes foresight and is crucial to better manage a firm's response to litigation. The eDIRT and the designated Attorney, e-Discovery coordinator, and the 30(b)(6) witnesses are a foundation that almost every company generating more than $7 Million dollars in revenue needs (Small Business Administration, 2015). The eDIRT should adhere to four principles 1) distribute litigation holds, 2) track custodians, 3) maintain documentation, and 4) collect relevant information (Aversano, 2015). The formalization of the Legal Hold processes to notify, track, and manage custodians across the company requires interaction and business process engineering between Human Resources, IT, and Legal departments. Equally important are the tasks to formalize the e-Discovery incident response team (eDIRT). The partnership with the Legal department and its Lit-support team alongside the IT/IS department is needed to be able to swiftly discern the identification, collection, and preservation of ESI.

At some level, litigation may be inevitable. An appropriate e-Discovery program can do a great deal to defend the enterprise. Establishing an organizational culture that values business records, treats each document as a record to be used, and treated in a reasonable manner though its lifecycle mitigates the effects of litigation though RIM. Data Governance and Records Information Management along with the e-Discovery Reference Model (EDRM) and its integration with Information Governance Reference Model (IGRM) can deliver a path to minimize litigation response while maximizing effectiveness.

The real challenge of addressing the over litigious business environment is not just juggling one more management task alongside of people, products, and profits (W.J. Sanders III, 2000). It is determining the proper direction for creating a practice of both offense and defense that works for the success of the company.

References

AdvantaCare Health Partners, LP v. AccessIV, No. 03-04496, 2004 WL 1837997 (N.D. Cal Aug 17, 2004).

American Bar Association. (2015, 05 27). *Step in a Trial*. Retrieved from How Courts Work: http://www.americanbar.org/groups/public_education/resources/law_related_education_network/how_courts_work/pleadings.html

Apple Inc. v Samsung Electronics Co. Ltd et al, No. 5:2011cv01846 (N.D. Cal 2012).

Association of certified e-Disocvery Specialists. (2014). *CEDS Examination preparation manual third edition.* Miami, Florida: ACEDS.

Blue Sky Travel & Tours, LLC v. Al Tayyar, 2014 WL 1451636 (4th Circuit March 31, 2015).

Bort, J. (2015, May 29). *CEO of bankrupt Linux company says employee lawsuits put it out of business.* Retrieved from Business Insider: http://www.businessinsider.com/ceo-employee-lawsuits-killed-mandriva-2015-5?op=1

Boudreau, K. (2010). Open platform strategies and innovation: granting access vs. devolving control. *Management Science 56(10)*, 1849-1872.

Carrillo v. Schneider Logistics, Inc., No. CV11-8557-CAS (C.D.Ca 12 31, 2012).

Chutich v. Papa John's International, Inc., No. C10-1139-JCC (W.D. Wa. 11 9, 2012).

Computer Research Association. (2012, Nov 30). *Challenges and Opportunities with Big Data.* Retrieved from www.cra.org: http://www.cra.org/ccc/files/docs/init/bigdatawhitepaper.pdf

Cornell University Law School. (2005). *Legal Information Institute*. Retrieved from Rule 26. Duty to Disclose; General Provisions Governing Discovery: https://www.law.cornell.edu/rules/frcp/rule_26 retrieved 6-1-2015

e-Discovery HQ. (2012, June 25). *e-Discovery Requirements*. Retrieved from http://ediscoveryhq.com: http://ediscoveryhq.com/ediscovery/ediscovery-requirements/ retrieved 7-6-15

EDRM (edrm.net). (2012, Oct 11). *Information Goverance Reference Model Version 3*. Retrieved from www.edrm.net: www.edrm.net/resources/guides/igrm retrieved 5-15-15

EDRM.NET. (2012, Oct 11). *Information Governance Reference Model (IGRM)*. Retrieved from www.edrm.net: www.edrm.net/projects/igrm retrieved 5-15-15

EDRM.NET. (2014, May 14). *EDRM Framework Guides Version 3*. Retrieved from EDRM Framework: http://www.edrm.net/resources/guides/edrm-frameworks-guides retrieved 5-30-2015

Gallagher, S. (2015, March 8). *The Ambassador who worked from a Nairobi bathroom to avoid State Dept. IT.* Retrieved from Ars Techica: http://arstechnica.com/information-technology/2015/03/the-ambassador-who-worked-from-nairobi-bathroom-to-avoid-state-dept-it/

Gartner Group. (2011, July 31). *Pattern-Based Strategy: Getting Value from Big Data July 2011.* . Retrieved from www.gartner.com: http://www.gartner.com/it/page.jsp?id=1731916 retrieved 6-7-2015

Gokare, P.C. v. Federal Express Corp., No. 11-cv-02131 (Western District of Tennessee 8 1, 2012).

Grayson v. Cathcart , No. 2:07-00593-DCN (2013 U.S. Dist Apr. 8, 2013).

György, A., Cleven, A., Uebernickel, F., & Brenner, W. (2012). Exploring the shadows: IT governance approaches to user-driven innovation. *ECIS 2012 Proceedings* (pp. paper 222 (1-13)). ECIS.

Healthcare Information and Management Systems. (2014). *Title 45 - Public Welfare. Subtitle A, SUBCHAPTER CPART 160, GENERAL ADMINISTRATIVE REQUIREMENTS.* Retrieved from Subpart A - General Provisions. 45 CFR 160.103: http://www.himss.org/files/HIMSSorg/Content/files/CPRIToolkit/version6/v7/D88_Special_Issues_and_Concerns(2).pdf

International Organization for Standardization - ISO. (2001). *ISO 15489-1:2001 - Information and Documentation - Records Management - Part 1: General.* Retrieved from www.iso.org: http://www.iso.org/iso/catalogue_detail?csnumber=31908

International Standardization Organization (ISO). (2001). *ISO 15489-1:2001 - Information and Documentation-Records Management Part 1: General.* International Standardization Organization (ISO).

ISC². (1992). *History of (ISC)².* Retrieved from www.isc2.org: https://www.isc2.org/isc2-history.aspx

Jackson, S. (2011). Rule 30(b)(6) Deposition Myster Revealed: What Records Professionals need to know. *ARMA International, www.arma.org November/December*, 27-30 .

Katherine Aversano, J. a. (2015, May/June). Avoiding the Hammer: Defensible Strategies for FRCP Proposed Rule 37. *Information Management*.

Koontz, H. &. (1955). *Principles of management. an analysis of managerial functions.* . New York: McGraw-Hill.

Kroll OnTrack. (2013, 09 26). *Sekisui Am. Corp. v. Hart: Judge Scheindlin's Latest Footprint in Spoliation Case Law – Part 2*. Retrieved from TheeDiscoveryBlog.com: http://www.theediscoveryblog.com/2013/09/26/sekisui-am-corp-v-hart-judge-scheindlins-latest-footprint-in-spoliation-case-law-part-2/ retrieved 6-5-15

Law.com. (2015, 07 07). *Basic Principles of Case Law*. Retrieved from Law: http://common.laws.com/case-law

Legal Hold Pro. (2014). *Legal Hold & Data Preservation Benchmark Survey 2014.* Legal Hold Pro and the Steinburg Group .

Logtale, Ltd. v. IKOR, Inc., 2013 WL 3967750 (N.D. Call July 31, 2013).

Mosaid v. Samsung, 348 F. Supp.2d 332,333, and 339 (D.N.J. 2004).

Murphy, B. (2011, 11 29). *e-Discovery in the cloud not as simple as you think.* Retrieved from http://www.forbes.com: http://www.forbes.com/sites/jasonvelasco/2011/11/29/e-discovery-in-the-cloud-not-as-simple-as-you-think/

Myers, N. a. (2015, March 9). *The Impact of Shadow IT Systems on Perceived Data Credibility and Managerial Decision Making* . Retrieved from Available at SSRN: http://ssrn.com/abstract=2334463 or http://dx.doi.org/10.2139/ssrn.2334463 retrieved 6-21-2015

NIST. (2012, August 31). *Computer Security Incident Handleing Guide*. Retrieved from NIST.SP.800-61r2: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf retrieved 6-5-15

Ohio Northern District Federal Courts. (2011). *Ohio Northern District Federal Courts Rules and Orders Local Civil Rules Appendix K.* Cleveland OH: Ohio Northern District Federal Courts.

Pelline, D. G. (1998, May 18). *Smoking gun in Microsoft memos?* Retrieved from CNET News: http://news.cnet.com/2100-1001-211315.htm

Reginald W. Jackson, E. (2012). *THE BURDENS OF TECHNOLOGY: ATTORNEY DUTIES IN THE ELECTRONIC AGE* . Retrieved from Southeastern Bankruptcy Law Institute: http://www.sbli-inc.org/archive/2012/documents/T.pdf retrieved 5-20-2015

Resolution Trust Corporation Fa v. Southern Union Company Inc, 985 F.2d 196, 25 Fed.R.Serv.3D 253 (United States Court of Appeals, Fifth Circuit Mar 5, 1993).

SANS CSC. (2015). *Critical Security Controls - Version 5*. Retrieved from www.sans.org: https://www.sans.org/critical-security-controls/ on 05-21-2015

Schuler, K. a. (2009). *E-Discovery creating and managing an enterprise program : a techincal guide to digital investigation and litigation support.* Syngress Pub.

Silvestri v. General Motors, 271 F.3d 583, 591 (4th Cir. 2001).

Small Business Administration. (2015, 07 14). *SUMMARY OF SIZE STANDARDS BY INDUSTRY SECTOR*. Retrieved from Small Business Size Standards: https://www.sba.gov/content/guide-size-standards-0

Sullivan, M. (2015, 07 17). *These 12 startups died in Q2. Here's why and how.* Retrieved from VentureBeat: http://venturebeat.com/2015/07/17/these-12-startups-died-in-q2-heres-why-and-how/

The Sedona Conference. (2013, December 31). *Commentary on Information Goverance*. Retrieved from https://thesedonaconference.org: https://thesedonaconference.org/publication/The%20Sedona%20Conference%C2%AE%20Commentary%20on%20Information%20Governance retrieved 6-5-2015 page 130

The Sedona Conference. (2015, April 30). *The Sedona Conference Commentary on Possession, Custody, or Control*. Retrieved from https://thesedonaconference.org: https://thesedonaconference.org/publication/The%20Sedona%20Conference%20Commentary%20on%

20Rule%2034%20and%20Rule%2045%20%E2%80%9CPossession%2C%20Custody%2C%20or%20Control%E2%80

The Sedona Conference Glossary. (2014, April 30). *E-Discovery and Digital Information management (Fourth Edition)*. Retrieved from https://thesedonaconference.org: https://thesedonaconference.org/download-pub/3757 retrieved 6-5-2015

Toshniwal, R. D. (2015). . Big Data Security Issues and Challenges. , 2(2). *Complexity Vol. 2*, 2.

Totenberg, N. (2014, 07 28). *When Did Companies Become People? Excavating The Legal Evolution.* Retrieved from National Public Radio: http://www.npr.org/2014/07/28/335288388/when-did-companies-become-people-excavating-the-legal-evolution retrieved 6-21-2015

U.S. Army. (1936). *George Washington University. "ATTACHMENT 2 AR 320-5, CLASSIFICATION OFC. Army Regulations (1936)"* . Retrieved from gwu.edu.: http://nsarchive.gwu.edu/radiation/dir/mstreet/commeet/meet14/brief14/tab_d/br14d1b.txt retrieved 07-07-2015

W.J. Sanders III, A. C. (2000, April 27). *2000 Annual Shareholders Meeting*. Retrieved from Jerry Sanders Speech at the Annual AMD Shareholders event: http://www.pcstats.com/releaseview.cfm?releaseID=198

West v. Goodyear Tire & Rubber Co., 167 F.3d 776,779 (2d Cir 1999).

Wikipedia. (n.d.). *Incident_Management*. Retrieved from https://en.wikipedia.org: https://en.wikipedia.org/wiki/incident_management retrieved 6-5-15

William W. Belt, D. R. (2012). Technology-Assisted Document Review: Is It Defensible? *Richmond Journal of Law & Technology Volume XVIII, Issue 3*, 1-6.

Withers, K. J. (2006, Spring). Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure. *Northwestern Journal of Technology and Intellectual Property Vol.4*, p. 171.

Wyatt, K. (2015, July 14). *Lawsuits are friends of pot opponents.* Retrieved from Durango Herald: http://www.durangoherald.com/article/20150714/NEWS04/150719823/0/News03/Pot-opponents-using-lawsuits-to-kill-industry-

Young, D. L. (2011). *A Primer on 30(b)(6) Depositions; A defense Perspective.* Retrieved from http://www.americanbar.org: http://www.americanbar.org/content/dam/aba/administrative/labor_law/meetings/2011/ac2011/134.authcheckdam.pdf

Last Updated: September 25th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS DFIR Prague Summit & Training 2017	Prague, CZ	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZUS	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, SG	Oct 09, 2017 - Oct 28, 2017	Live Event
Secure DevOps Summit & Training	Denver, COUS	Oct 10, 2017 - Oct 17, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VAUS	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, JP	Oct 16, 2017 - Oct 28, 2017	Live Event
SANS Brussels Autumn 2017	Brussels, BE	Oct 16, 2017 - Oct 21, 2017	Live Event
SANS Berlin 2017	Berlin, DE	Oct 23, 2017 - Oct 28, 2017	Live Event
SANS Seattle 2017	Seattle, WAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS San Diego 2017	San Diego, CAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, AE	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Miami 2017	Miami, FLUS	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Milan November 2017	Milan, IT	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Amsterdam 2017	Amsterdam, NL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Sydney 2017	Sydney, AU	Nov 13, 2017 - Nov 25, 2017	Live Event
Pen Test Hackfest Summit & Training 2017	Bethesda, MDUS	Nov 13, 2017 - Nov 20, 2017	Live Event
SANS Paris November 2017	Paris, FR	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CAUS	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, GB	Nov 27, 2017 - Dec 02, 2017	Live Event
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZUS	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Khobar 2017	Khobar, SA	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Munich December 2017	Munich, DE	Dec 04, 2017 - Dec 09, 2017	Live Event
European Security Awareness Summit & Training 2017	London, GB	Dec 04, 2017 - Dec 07, 2017	Live Event
SANS Austin Winter 2017	Austin, TXUS	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Bangalore 2017	Bangalore, IN	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Frankfurt 2017	Frankfurt, DE	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DCUS	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Oslo Autumn 2017	OnlineNO	Oct 02, 2017 - Oct 07, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced