Spring 2008

Developing a Proactive Framework for E-Discovery Compliance

Gerald L. Wallner
Regis University

Regis University
College for Professional Studies Graduate Programs
Final Project/Thesis

Disclaimer

Developing a Proactive Framework for E-Discovery Compliance

By

Gerald L. Wallner

A Thesis/Practicum Report submitted in partial fulfillment of the requirements for the degree of Master of Science in Computer Information Technology

School of Computer & Information Sciences
Regis University
Denver, Colorado

April 15, 2008

Chapter 1

Abstract

Wallner, Gerald L. MSCIT Program. School of Professional Studies, Regis University, Denver Colorado. April 9, 2008. Developing a Proactive Framework for E-Discovery Compliance. Instructor: Donald Archer. Project Advisor: Paul Vieira.

The purpose of this document is to provide Information Systems Management an awareness of a compliance risk associated with the management of electronic data. The changes to the Federal Rules of Civil Procedure in 2006 make electronic data discoverable as evidence for civil court cases introducing the need for proactive management of end user data beyond the data that a particular form of legislation may require. Leveraging existing forensic data collection processes and raising the awareness of the problem and risk to the organization will provide a level of assurance for compliance should the data be requested in a civil trial. This project analyzed the current state that existed for businesses and organizations, the actual risk and precedence that has been set, and determines the current state of awareness and readiness that businesses have for this problem. The project then offers a solution to this problem that will aid in reducing the risk and hardship an organization could face when electronic data is requested. Finally, this project presents the results of actual testing of the proposed solution in a real world business enterprise.

Acknowldgement

I would like to acknowledge the support of my family, friends and colleagues during this project. I also extend sincere appreciation and thanks to my project advisor Paul Vieira for his time, feedback, and encouragement during this project.

Table of Contents

Chapter 2

The Problem Statement

In December of 2006 the Federal Rules of Civil Procedure (FRCP) which provide the framework by which civil cases are handled within the court system, were amended to include provisions for the discovery and subpoena of electronic records. Termed Electronic Discovery or *E-Discovery*, a new vulnerability has been exposed for the business in terms of how data is managed within the enterprise. The lack of application of standard forensic practices in the collection of this data results in significant burden and risk for an organization when it is required to provide the data requested to a court of law.

With past violations of specific legislative Acts, the penalties were based on the criminal court system. With the movement of the risk into the civil court system, awards by jurors to plaintiffs for E-Discovery violations have ranged as high as the $1.58 Billion imposed on the investment banking firm JP Morgan Chase (Hartwig PhD et al., 2007) to a comparably low $2.75 Million imposed upon Phillip Morris (Lang & Baffa, 2007).

Thesis Statement

The implementation and application of computer forensic analysis practices and data collection tools can reduce the burden and risk for an organization when required to provide data requested by a civil court.

Project Need Statement

The need for managing end user data has never been more important than the present. With the recent changes to the Federal Rules of Civil Procedure (FRCP) in December 2006

which define how the federal courts conduct civil cases with many state court systems following suit in their own processes, the FRCP defined procedures for requesting electronic records as part of civil court system (Cornell Law School, 2007).

While information related compliance has generally been left to specific regulatory legislation such as the Code of Federal Regulations (CFR's) for the pharmaceutical industry, and the Sarbanes-Oxley Act for finance and accounting record keeping, these changes in the FRCP have moved compliance out of a specific legislative directive to a case argument or Tort and it is anticipate that legal practitioners such as the plaintiff's bar will attempt to leverage these changes to set new precedents within the Civil Tort system within the United States federal and state courts (Hartwig PhD et al, 2007).

Where traditional computer forensic analysis practices have centered on evidence gathering for criminal cases based on intrusion, damages caused to a target organization's data or networks, E-Discovery now poses a dilemma for an organization in forecasting possible litigation prior to any action or activity actually occurring. Extending beyond the current forensic practices that exist, management of end user data now becomes not just a topic of knowledge management, but also compliance management.

Project Research Methods

The management of large volumes of data has always been a problem for businesses and organizations, there are also many existing practices, methods, standards and criteria such as those presented by the International Organization on Computer Evidence (IOCE) that may be leveraged and adapted to solve this particular problem. Research for the project leveraged existing industry best practices to adapt those processes, or to formulate new processes that will aid in solving the problem of E-Discovery compliance (Yeager, 2007).

Research Focus:

1. Chapter 1 provides the project abstract.
2. Chapter 2 provides the project problem statement, thesis, hypothesis, need for the project, and discussion of the subsequent chapters and how they support the project.
3. Chapter 3 covers the review of the literature and current body of knowledge including existing case studies and industry best practices associated with criminal forensic analysis.
4. Chapter 4 covers the gathering of survey data and statistical analysis of the data to support the thesis.
5. Chapter 5 assesses the current technology and software that is best suited to solving the problem.
6. Chapter 6 provides an architecture model for implementation of a data collection process including establishment of policies and procedures to support the collection activity such that the policy itself may serve as a defensible argument for undue hardship (Lexis Nexis Federal Rules of Civil Procedure, 2006).
7. Chapter 7 covers the synthesis of the data and analysis of the results in relation to the proposed solution.
8. Chapter 8 summarizes the project and conclusions.
9. The appendix includes references, table of figures, and an annotated bibliography.

Project Completion

With the existence of electronic data, the issue of E-Discovery will be with us as long as electronic data exists and there is no foreseeable end to the collection of electronic data in our lifetime. The project at completion presents the problem as it exists currently, and a solution to reducing that risk. Forensic analysis practices, tools and techniques were researched during this project for applicability as a solution to this problem. Knowledge management practices and data classification methods were also researched. Current statistics and case studies were gathered and evaluated. The project completed with the development of an architecture model for data collection of distributed data to fulfill E-Discovery compliance.

Project Background

Regulatory compliance in the pharmaceutical industry is a fact of life in order to provide assurance that the products that are manufactured are safe for the patient. This entails the need for explicit documentation practices, data management and protection of proprietary knowledge, and standard operating procedures to ensure the consistency in the operations and product manufacturing process. Much of the requirements that exist are regulatory in nature where the law mandates what must be done, when, and how, such that a framework for organization of electronic data relating to product is provided for us. However; with the advent of the FRCP changes of 2006, the management of data has moved from an explicit and prescribed requirement, to that of needing to identify exactly what must be collected and managed before it is actually requested. If this can be problematic for an organization focused on data collection and compliance, it can be far worse for organizations not currently required to maintain this level of organization with end user data. As such, it provides a relevant and intriguing problem area for a solution.

How these areas apply to this project

Knowledge Management begins with the capture and management of data such that it becomes information. The principles of Knowledge Management provide the basis for data collection. Information Security has traditionally focused on protecting the enterprise from intrusion or malicious attack and forensic analysis has traditionally been applied to criminal investigations. However; the forensic analysis practices can be applied as an aid to the collection process to provide assurance of data integrity. Architecture Design develops a framework from which to operate in whether it is software development or systems implementation, a system is not necessarily a computer system rather; can also be a practice, service or collection of services. With any architecture or proposed implementation, the model must be feasible and deployable in an organized manner denoting the importance of Project Management.

The Scope of this Project

The project focuses on the application of traditional information security forensic collection practices, techniques, and theory to aid in the collection of end user data stored on local hard drives such that the data is retrievable by legal professionals within a Fortune 500 pharmaceutical company. The project assessed the awareness level for this problem across many industries, proposing a framework for collection of hard drive data in a Fortune 500 pharmaceutical company and assessed the effectiveness of the solution implemented towards solving this problem. The project further explored new problems created by this new risk in the enterprise and identifies data through survey results to assert that many enterprises already have the core capabilities and tools necessary to enable compliance with E-Discovery for their businesses.

The scope of the project activity was to aid in the selection of a collection tool and development of a design model for the method of collection for end user hard drive data. The actual testing activity was conducted over a four month period at one of the Fortune 500 pharmaceutical company's North American locations.

Chapter 3

Review of the Literature and Research

The literature gathered in support of the project and hypothesis has been assembled from professional journal publications, professional book publications, and direct technical references relating to the topic. This body of knowledge presents such topics as specific definition of how the civil court process originated and is currently defined at present; industry best practices associated with forensic data collection and analysis techniques; case references for existing cases directly related to the topic of electronic discovery.

At present, the risk and liability associated with electronic discovery of data as part of the civil court procedure is unfolding with precedence being set within the Unites States court systems since December of 2006 to present. What is known is that company's face a new liability risk in relation to how data is collected, requested and retrieved for civil litigation.

It is this author's objective to present a framework by which existing forensic collection practices can be applied to the problem of data collections for E-Discovery compliance such that organizations within the industry may leverage existing tools and practices to solve this problem and minimize the risk and liability that could be imposed for failure to properly collect end user data from personal workstations equipment in support of litigation activities.

From the beginning of the twentieth century as the industrial revolution continued to expand, there was an increase in liability suits within the civil court system referred to as torts which deal with wrongful acts and the liability that is incurred through those acts. Cases ranged from liability claims from on the job injuries to defective merchandise that caused the consumer harm and imposed liability for parties that placed other parties in possible harms way such as injuries at company picnics and parties. Other cases stemmed from the practices of companies settling with potential plaintiffs out of court for injuries or wrongful death where plaintiffs would be paid anywhere from $75 to $1000 depending on social class, race, and the likelihood that the potential plaintiff could actually afford to bring a case to civil court (Friedman, 2007).

As the complexity of manufacturing goods were combined with the complexity in such good's operation, the original complaints were based upon negligence in manufacturing however; this has evolved to a principle to make a company pay for what it's product does as an end result regardless of whether or not negligence in manufacturing played a part or not. This has moved the civil liability to focus upon the end result or outcome rather than in the process itself. As these cases evolved and gained momentum is the civil court system, it became easier for people and the court system in the United States to accept the idea of product liability such that the principle that companies who make product must bear the responsibility and accountability for those products when they ultimately cause harm to the consumer (Friedman, 2007).

As laws and case precedents evolved over the twentieth century, some industries actually found their activities regulated under more stringent legal requirements under Federal laws where violations were not only tort risks, but criminal prosecution could be imposed as well. This led to the principle of compliance in fulfilling these responsibilities. Compliance initially

stemming from the United States financial enterprises indicates the observance of norms within the organization to include observance of legislative Acts, industry standards, directives, statutes and in also the behavioral aspects of the organization with regard to ethics (Gasser & Haeusermann, 2007).

Compliance is defined by Gasser & Haeusermann (2007) as "the management of risks at the intersection of law, technology, and the market" where compliance is now regarded as an element of risk management for a business enterprise (p. 17).

With the advent of the information age, it was inevitable that the tort system would eventually realize the wealth of information that could be discovered as part of civil litigation discovery processes. However; electronic information is far different than paper based flat file systems and new rules would need to be defined for how to handle discovery of this kind of data. On December 1, 2006 such rules amendments went into effect for the Federal Rules of Civil Procedure (FRCP) which were first enacted in 1938 to define the practices, principles, and rules by which attorneys and litigators conduct their cases within the United State Federal civil court system (CommVault Solutions Legal Discovery, 2007). Termed E-Discovery, the new amendments to the FRCP set the ground rules that attorneys must follow in pursuit of discovery of electronically stored information and while local state courts are not bound by these principles; state courts often look to the FRCP as guidance in establishing their own rules for civil litigation (Hartwig PhD et al, 2007).

The primary rules amendments were made on rules 34(a) (b), 26(f) (b) (B), and rule 37(f). Each of these rules provides specific procedures relating to the archival, data protection, resource management, request methods, identification of discoverable documents, establishment of agreement on format types, and justifications for what is defined as a hardship or loss of data

in good faith efforts in the course of normal business practice (Cornell Law School Federal Rules of Civil Procedure, 2007).

The types of data that have been found to fall within the scope of Rule 34's data compilation definition include e-mails, data processing cards, input data, backup tapes, databases, voicemail, text messages, Internet usage histories, instant messages, and electronic document files all discoverable on a wide range of computing technologies including personal computers, servers, personal digital assistants (PDA's), pagers, cell phones, optical disks, flash media thumb drives, and backup tapes to name a few (Lang & Baffa, 2007).

While E-Discovery costs may be significant in some cases, the cost for non-compliance may be far more expensive where the consequences for failing to comply with E-Discovery rules may result in monetary sanctions imposed by the court, influence of the jury's perception of the defendant, and default judgments against a plaintiff (Hartwig PhD et al, 2007).

The damages that have already been established in legal case precedents include Zublake vs. UBS Warburg LLC (S.D.N.Y. 2004) for $29 Million where jurors awarded damages in a discrimination case where the failure by the defendant to produce e-mails requested were cited to contain information detrimental to the defendant's case; Coleman Holdings vs. Morgan Stanley & Co., Inc. (Fla. 15th Jud. Cir., 2005) for failure to search for and provide thousands of e-mail backup tapes that could prove that the defendant attempted to defraud investors resulting in a judgment of $1.4 Billion in compensatory damages to the plaintiffs; Kucala Enterprises Ltd. Vs. Auto Wax Co. (N.D. III. 2005) where the plaintiff destroyed electronic documents with a software program titled *Evidence Eliminator* following a counter claim suit and discovery request by the defendant where the court imposed sanctions, attorney's fees and other expenses

on the plaintiff and informed the jury to consider the electronic document destruction in the counter-claim brought by the defendants (Lang & Baffa, 2007).

Where corporate defendants shudder when E-Discovery is mentioned, in other cases corporate defendants are serving E-Discovery requests against the plaintiffs in civil cases as the rules apply both ways and E-Discovery can provide significant discoverable information about a plaintiff's injury, earning capacity, life style, employment history, and education (Probst & Wright, 2006). This data can provide key information regarding the plaintiff's intent and objectives in a case and even discredit the case resulting in an out of court settlement or dropping of the case all together. Probst & Wright (2006) recommends that council should know "what to ask for" in deposition outlines in order to identify key discoverable electronic information such as e-mail; e-communications such as instant messaging and chat logs; electronic appointment books, cell phone information and billing statements; how many computers the plaintiff owns and uses; screen names; and Internet Service Providers [ISP's] (P1).

Lawyers tend to overestimate their level of recall in regard to E-Discovery and with the unprecedented size and scale of electronic data that can be subjected to an E-Discovery request during litigation, the ability to efficiently gather these large sets of electronic data can pose a challenge for and organization (Baron & Thompson, 2007). Maintaining the efficacy of that data also poses a challenge especially in the beginning of the process. One of the greatest violations that can occur with E-Discovery will occur right at the beginning of the process where IT personnel and legal professionals may become so focused on getting the data, they begin turning on systems to begin data mining documents. The risk imposed at this early stage lies in powering on the system itself. Powering up and logging onto systems may alter, overwrite,

modify, or change the state of the system such that the evidence collected may come into question regarding its efficacy and validity (Burke, 2007). Fulfilling the need for computer security professionals properly trained in computer forensic practices and methods is essential to alleviating some of these early mistakes.

This application of standard computer forensic practices can alleviate this risk. "Computer forensic is the identification, preservation, and the analysis of information stored, or produced by a computer system or computer network" (Francia & Clinton, 2005, p. 144). "Computer forensic science is the science of acquiring, preserving, retrieving, and presenting data that has been processed electronically and stored on computer media" (Yeager, 2006, p. 168). When considering the objectives of E-Discovery in comparison to the activities and definition of computer forensics, the same principles used in collection, acquisition, analysis and preservation of data for criminal cases also provides the framework for the management, operational and technical controls used within information security to be applied to E-Discovery collections (Yeager, 2006).

For many businesses and enterprises, much of the technology, operations, and capabilities may already exist to solve the e-discovery collection problem for the desktop computer.

Chapter 4

Survey Data

In support of this project, an electronic survey was conducted to assess the awareness level, capabilities and technologies that exist within business IT enterprises to support or disprove the assertion that the technology for solving the E-Discovery desktop computer collection process already exists in many business enterprises. The survey of ten questions was conducted across a diverse range of business enterprises ranging from small, medium, and large

businesses in a diverse sample of industries ranging from information technology companies, insurance companies, and government agencies. The target respondents were selected from a list of IT professionals working within these industries. The survey responses were kept simple with *yes, no,* or *don't know* answers. To maintain the survey as a blind survey, respondents were provided a hyperlink to access the electronic survey through the Zoomerang (www.zoomerang.com) web survey service. With exception to the size of the business enterprise as reported by the respondent, no method for identifying the individual respondents or companies they work for was attached to the survey to maintain each respondent's confidentiality and non-disclosure risks that might relate to their individual obligations to the businesses and organizations they work for. Out of approximately sixty solicited participants, one third of the respondents solicited responded to the survey totaling twenty responses. The survey results reflect these participant's responses to the survey questions.

The definition of a small, medium, or large enterprise was defined from Microsoft's Solution Finder Partners Directory (2008) where a small business was defined as 1-49 employees, a mid-market or medium business was defined as 50-1000 employees, and an enterprise business or large business was defined as over 1000 employees.

Over a year after the institution of the revised Federal Rules of Civil Procedure, Chris Preimesberger (2007) cites in his article for Ziff Davis that "two thirds of U.S. businesses remain unprepared to meet strict court requirements for the discovery and handling of electronic evidence" (p. 1). Question 1 of this survey asked respondents: *Have you heard the term E-Discovery or Electronic Discovery?* Of the responses, 70 percent cited '*no*' answers, 30 percent cited '*yes*' answers and none reported '*don't know*'. This statistic falls in alignment with Preimesberger's assertion that two thirds of businesses are unaware of this problem and risk.

To determine that the survey was conducted across a cross section of business enterprises, the second question asked the respondent: *What is the total number of employees in your business?* Of the responses provided, 21% percent fell within the small business criteria of 1-49 employees; 37 percent fell into the medium business criteria of 50-1000 employees; and 42 percent fell within the large enterprise or large business category of over 1000 employees. These numbers illustrate that a fairly even cross section of business enterprises responded in terms of size of the business or organization with the heaviest number of responses associated with the large business category.

The 3rd question in the survey was designed to assess the number of employees in the organization that actually use a computer as number of employees alone does not necessarily mean that data is generated on a personal workstation computer for some business enterprises. The responses to the question: *How many employees in your business use a personal computer?* Revealed that 20 percent responded 1-49; 35 percent responded 50-1000; and 45 percent responded over 1000 denoting that the number of employees within the organization reported in question number 2 did in fact use a personal computer in their job.

The next series of questions were designed to assess the potential that the technologies and business practices already exist within these organizations to address the E-Discovery collection issue. Question 4 asked: *Does your enterprise have a method for storing end user data files on servers?* There was overwhelming response with 90 percent of the respondents citing '*yes*' and only 10 percent citing '*no*' to this question illustrating that centralized server based storage has become a norm of most businesses. This also illustrates that the capability

exists for collection of end user data during an E-Discovery request from these centralized locations.

While storing this data may be of benefit to the enterprise operation, risk of discovery associated with storing vast amounts of legacy data can pose a problem for a business. As a result, the Federal Rules of Civil Procedure encourage a company to establish or have a clear data retention policy (Preimesberger, 2007). Question 5 of the survey was designed to determine how many enterprises have a data retention policy in place by asking: *Does your enterprise have a data retention policy?* The responses to this question revealed that 85 percent of the respondents answered '*yes*' to this question; 10 percent answered '*no*', and 5 percent responded as '*don't know*'. Chris Preimesberger (2007) cites in his article for Ziff Davis titled "Businesses Generally Ignoring E-Discovery Rules" that "53 percent of companies lack a policy governing e-mail retention and deletion"; 67 percent of companies allow individual end users to determine how long messages are kept by the company"; and 66 percent of companies do not have the e-mail archiving technology required to manage e-mail retention, litigation holds and e-discovery" (p. 2). This suggests a disparage between this survey and Preimesberger's however; the context and scope of a data retention policy may can be extensive and detailed such as those implemented within businesses subjected to regulatory requirements that mandate retention of data versus those defined by a business for maintaining data for business continuity and operational knowledge. What the survey statistic for this project does illustrate is that 85 percent of the respondent's business enterprises do have a familiarity and process for establishing and maintaining some form of data retention policy.

Question 6 was designed to assess how many business enterprise's IT operations utilize some form of hard drive duplication technology by asking: *Does your Information Technology*

utilize any form of hard drive snapshot or imaging technology for capturing and deploying pre-built hard drive configurations? 70 percent of the respondents answered '*yes*'; 20 percent answered '*no*' and 10 percent answered '*don't know*'. The answer to this question was of particular interest to this project in determining the capability for an enterprise to leverage existing hard drive duplication software and technologies for data collections in fulfillment of E-Discovery requests.

While the focus of this project targets the data collection issue for the personal computer workstation and laptop technologies, many of these systems are used for accessing, downloading, and working with documents and electronic data from centralized data repositories such as document management systems, data warehouses, and knowledge management systems in general. As the electronic data stored within a knowledge management system, question 7 asked: *Does your enterprise have a document management system?* 60 percent of the respondents answered '*yes*' to this question; 25 percent answered '*no*'; and 15 percent answered '*don't know*'. Bercerra-Fernandez, Gonzales & Sabherwal (2004) in their book "Knowledge Management Challenges, Solutions, and Technologies" defines a document management system as "essentially storing information" where "a document management system unifies and aggregate of relevant information conveniently in one location through a common interface or central repository" (p. 213). The statistic from our survey then presents that discovery of electronic information can be relatively easy for enterprises that have such central repositories where legal professionals may access the documents requested in an efficient and timely manner however; the 25 to possible 35 percent of respondents that did not have a document management system or were unaware of such a system in their enterprise denotes a higher risk potential that electronic documents created by an end user on their personal computer may actually be retained

on that individual system making discovery more difficult and necessitating that collection of that localized data is essential to maintaining E-Discovery compliance.

How does an IT organization go about identifying and reclaiming such information? Question 8 targeted this problem by asking: *Are employee's personal workstations / laptops reclaimed by your IT department for redistribution when an employee leaves the company employment?* 85 percent of respondents answered '*yes*' to this question; 15 percent answered '*no*' and no respondents answered '*don't know*'. This denotes that for a large percentage of business enterprises, a mechanism or method for reclaiming this hardware exists where the IT organization within that enterprise knows where to get the system, reclaims the system, and processes it in some way for redistribution in the enterprise. This statistic was of important in identifying the capability to reclaim hardware as our project will illustrate in subsequent chapters the importance of system reclamation in the chain of custody process for E-Discovery.

While question 8 of the survey determine the percentage of respondents whose enterprise reclaimed personal computer equipment for redistribution within the company; question 9 sought to understand what IT does with the equipment once it is in their hands by asking: *Do you quarantine the desktop / laptop of an employee that left the company to preserve the data for any period of time*? 25 percent answered '*yes*' to this question; 45 percent answered '*no*'; and 30 percent answered '*don't know*'. Given the 70 percent lack of awareness of E-Discovery cited in question 1 of the survey combined with this response statistic, the 30 percent that responded as '*don't know*' can be interpreted as a lack of awareness of the data preservation requirement within their respective enterprises or that their organizations have no policy for quarantine of an individual personal computer workstation. This suggests that between 30 to 55 percent of business enterprises may be at risk in their ability to fulfill the *good faith* effort toward

preserving data as specified in Rule 37's safe harbor provision for routine operation of the company's electronic information systems and more importantly, their ability to suspend those routine operations when an E-Discovery request is received (Shelton, 2006).

The final question of the project survey was designed to assess the potential that exists within a business enterprise to properly deal with E-Discovery compliance through properly trained IT personnel with the skill sets devoted to handling electronic evidence and computer system forensic analysis. Question 10 asked: *Does your enterprise have an information security function or use any forensic data collection practices for investigating personal workstations or laptops?* 30 percent of respondents answered '*yes*' to this question; 40 percent answered '*no*'; and 30 percent answered '*don't know*'. Given these results, we first must consider that where the 30 percent '*don't know*' answer is concerned, information security can often be considered a perimeter services function dealing with protecting the network infrastructure against intrusion thus, not well known by most users within an enterprise. Also, size of an enterprise can denote the presence of an information security function. And finally, as information security computer forensics has been mostly applied to criminal investigations in the past, confidentiality associated with most investigations would account for a lack of knowledge surrounding the presence of an information security organization within an enterprise unless a person was directly affected or participated in an investigation. This said, as our survey targeted IT professionals within their respective organizations; generally IT personnel will be more aware of the presence of an information security function within their company than most end users as in the ideal Infosec program, response and reporting methods for violations, risks and vulnerabilities will have been established. What our survey does illustrate is that a low percentage of enterprises may have the necessary skills sets to properly handle electronic evidence such that the efficacy of the data and

the chain of custody process could come into question with regard to the electronic evidence itself.

Browning Marean (2007) wrote in a paper for the New Jersey Law Journal titled "E-Discovery looks like risky business", "A significant challenge facing the profession is the need to attain sufficient competence to deal with the many deep complexities surrounding EDD [Electronic Data Discovery] though unfortunately, many attorneys are unaware of that complexity and could charitably be described as technologically challenged" (p. 1). Many of the mistakes that can occur in the E-Discovery process will occur early in the process beginning with the legal hold process placed on the data. Failure to enact a legal hold on the data in a timely manner can ultimately end a case before it has begun. Other risks that affect attorneys when dealing with E-Discovery requests lies in the ability to actually find and locate the data requested even to the point that courts have imposed sanctions on attorneys for failing to identify all of the information sources relevant to their cases (Marean, 2007). What this project's survey has revealed is that many business enterprises have the technology and capability to address E-Discovery compliance however; awareness of the problem is very low compared to the potential risk that exists.

When it comes to addressing the discovery of electronic information, application of traditional information systems forensic tools and practices, establishment or modification of information systems policies; following information systems security forensic science with regard to documentation and chain of custody; can aid an organization in their compliance with E-Discovery requests with the tools they have in house. "With proper attention to detail and documentation, there is no real reason to trip over the digital chain of custody" nor is their any real reason to trip over the E-Discovery process (Burke, 2007, p. 3).

Chapter 5

Review of the Software and Technologies

To apply information systems forensic tools and practices to this project, it was important to first identify what those tools and practices would be. As with any project, leveraging the System Development Life Cycle [SDLC] model best practices play an essential role in the successful implementation of any system whether it be an information system or a work system. In referencing the five phases of the SDLC, some of the key elements that had to be considered in addressing a process and tools for E-Discovery collection of computer workstation data included these elements from the initiation and planning phases of the SDLC as presented by the National Institute of Standards and Technology [NIST]:

- "**Risk Assessment** – analysis that identifies the protection requirements for the system through a formal risk assessment process. This analysis builds on the initial risk assessment performed during the Initiation phase, but will be more in-depth and specific." [From the Initiation Phase].
- "**Cost Considerations and Reporting** – determines how much of the development cost can be attributed to information security over the life cycle of the system. These costs include hardware, software, personnel, and training."
- "**Security Planning** – ensures those agreed upon security controls, planned or in place, are fully documented. The security plan also provides a complete characterization or description of the information system as well as attachments or references to key documents supporting the agency's information security program (e.g., configuration management plan, contingency plan, incident response plan, security awareness and training plan, rules of behavior, risk assessment, security test and evaluation results,

system interconnection agreements, security authorizations/accreditations, and plan of action and milestones)."

(Grance & Stevens, 2004, p. 5)

These phases were most essential in identifying specifically what the risk to the business was; any costs that would be incurred in the process to establish necessary budget allocations; and finally what controls would be put into place for the legal hold collection activity for the computer workstations to be collected from.

During the risk analysis phase, the project had to understand the process for E-Discovery request which breaks down into multiple steps once a lawsuit has been filed with the court:

- Legal Hold Phase- is initiated when council believes there is risk of litigation or a civil suit is likely such that all data retention and destruction policies surrounding a data type associated with a business practice or individual employee in the organization are suspended (Hill, 2006).
- Pre-discovery Phase- Opposing sides meet and negotiate the scope and depth of the information being requested as well as the format in which the information will be produced (Hill, 2006).
- Collection Phase- The defendant begins searching for the requested information in both paper and digital formats and initiates collection orders to IT and management staff, collects the data and begins analyzing the data and converting it into the agreed upon format (Hill, 2006).

The ability to locate the information can be difficult depending on how organized the defendant is with regard to managing data in their enterprise. Centralized file servers, e-mail servers and document management systems are much easier to locate because of their centralized

location however; locating a personal computer workstation or laptop can be very difficult in a large enterprise unless some form of asset management system is in place which ties the piece of equipment to the end user and the location where that end user resides. Use of some form of asset tracking will enable the IT personnel to quickly locate a unit and return it to a controlled location for collection of the data.

Gottschalk et al. (2005) cites that "criminals using computers may leave some evidence of their activities on their computers; seizing and analyzing such digital evidence has become an important aspect of criminal prosecution" (p. 147). This same philosophy applies to collections for E-Discovery and as the same information systems forensic practices can be employed for data collections for legal holds, the same tools will also be applicable to the E-Discovery collection process as would be used in a criminal investigation. In addition to the computer to be collected from, other tools will be necessary such as the following:

- Digital Camera- is a good tool for capturing the physical state of evidence in regard to damage to the computer prior to and after analysis.
- Screwdriver- is an essential IT tool in general and a screwdriver with multiple types of bits and head sizes can aid the forensic analyst in removal of parts, peripherals and drives from the computer workstation.
- Flashlight- is a tool that can be often overlooked until it is needed. The inside of computer cases can be quite dark and given the placement of devices and components can cast shadows over your work making reading jumper settings, pin configurations, or other critical information very difficult.
- Dremel Tool- is very useful in cutting screws that have stripped heads free from the casing or cutting other mounting brackets and small metal pieces.

- Extra Jumpers- are something that should be including as a critical component of any forensic analysis kit as it may be necessary to change the hard drive assignment such that it can be recognized when booted to another source such as changing a master drive to a slave in an IDE configuration, or assigning a different SCSI channel assignment to avoid a conflict between drives in the same chain.
- Extra Screws- are needed as you often do not know what condition a system will be in when you open it up and a previous technician may have taken some shortcuts leaving some of the screws missing. It is a good idea to replace any missing screws for mounting hard drives and other components such that those components do not come loose causing internal damage to the peripherals when the unit is transported back to storage.
- Cable ties- can come in very handy for securing cables and wiring that tends to get in your way when attempting to work with the components in the tight confines of a system casing.
- Internal Computer Power Extension Cords- may be needed to connect a removed drive to the forensic workstation for collection and analysis.
- Extra IDE and SCSI cables- come in real handy when connecting the drive to another workstation such as the forensic workstation or extending the range of the ribbon cable as many manufacturers may use the shortest cables to keep the internal case neat while saving costs in manufacturing in the shorter cable lengths.
- Documents- such as chain of custody forms, evidence labels, agent notes, and other evidence worksheets are not only essential to documenting what the forensic analyst does with the computer but those documents are evidence and discoverable in and of themselves.

- Evidence tape- often after a computer has been reclaimed for collection, placing some form of seal on the case cover can alert the forensic analyst to any tampering that might occur with the unit. In extreme cases, many computer workstations have a locking mount for a padlock or security cable to pass through such that numbered banding tags can be used to secure the case from being opened unless under proper conditions and chain of custody procedures.
- Anti-static bags- are an essential component for placing removed hard drives into as electrostatic discharge can cause severe damage to component circuitry and the cost to have a hard drive cracked open for a data retrieval by a professional service can be quite costly especially if cause by carelessness in handling the component resulting in its damage.
- Evidence Hard Drives- when reclaiming large volumes of data, the need for a target storage device to house this information may be necessary.
- Boot Floppies or Drives- As the act of booting a system can change or modify it's state by the simple act of booting the system up; external boot devices such as flash media disks where USB support is present, bootable CD / DVD ROMS, or external hard drives can allow the forensic analyst to boot to their operating system and access the target system's information with minimal risk of accidental modification.
- Network Hub / Switch- can be very useful in situations where network server resources are available and the data or disk duplication can be sent to a network repository.
- Power Strips- having a spare power strip is essential when the number of available power outlets are limited especially if a collection must occur in the field environment.

- Software- in addition to this kit, software installation media for multiple operating systems revisions and service packs may be needed; the ability to access alternative file formats such as NTFS may require specialized tools to see these drives through external sources, and of course in a collection process having a hard drive duplication application can allow capture of the contents of the drive without modifying the original data such that the state and contents are preserved within the hard drive image snapshot itself.

(Jones & Bejtilich, 2006)

As some forensic engagements may have some random element, problem, or facet that must be resolved in order to successfully perform a hard drive duplication such as errors on the target hard drive or other peripheral failures; having a complete forensic kit as listed can save the analyst considerable time and effort in dealing with the problem in a *forensically sound manner* and a forensic toolkit will need to contain nearly every conceivable peripheral interface and tool that one can think of (Jones & Bjtilich, 2006).

For this project, many of these tools were used with particular emphasis on leveraging network resources and file server storage, external boot capability, and hard drive duplication software. Of the software tools evaluated for this project, two in particular were evaluated and tested for their application to the legal hold collection process. The first was the Microsoft User State Migration Tool 3.0 (Microsoft Technet, 2008) however; two problems existed with this tool. The first was that the tool required the analyst to run the tool within the operating system session of the target machine risking alteration of the state of the machine by the mere nature of running the tool for collection. The second issue observed was that while the tool was able to collect the end user's documents and settings folders and their contents, the software ignored application loaded on the machine including the operating system itself. While poses a far less

storage footprint in terms of the amount of electronic information collected, it also poses risk of missing critical evidence that may be contained within the Windows Registry hives creation dates for installed applications themselves, etc.

The second tool evaluated was Symantec Ghost which allowed for full duplication of the target hard drive and allowed this collection to be captured via a remote bootable source such as a PE [Pre-installation Environment] bootable kit on a USB flash drive. This avoided any risk of accidental modification of system files, date stamps, modified dates, or other stately information such that the hard drive image collected maintained it's state information at the last time the unit was powered down and placed transported into the controlled environment where it was placed under quarantine.

In considering the order of volatility for the risk in accidental alteration or modification of the data such as logging onto the system creating entries into the system log files (Adelstein, 2006); it is best to boot the system with an external boot device such as a boot floppy, bootable CD, or a PE Bootable flash drive. One of the best tools for this purpose is the Bart's Preinstalled Environment [Bart PE] application which will allow the creation of a custom bootable Windows environment including any executable applications desired such as diagnostic tools, forensic analysis tools, and hard drive imaging applications. (Lagerweij, 2000-2008). This tool when used with a CD / DVD Bootable system, or preferably a flash memory stick configured for FAT32 for systems that support USB bootable capability; can boot the system and with the appropriate tools installed enabling access to the local hard drive without that local OS needing to boot up. This eliminates any unnecessary data stamps or modifications to the local system yet access to that system drive for copying data. Of the many hard drive imaging tools that may be leveraged, this project found that Symantec's (2004) Norton Ghost application for imaging hard

drives was preferred as used in conjunction with a PE Bootable, Norton Ghost provides a tool that may be preconfigured with a script file that automatically maps the target server volume; allows for network login authentication through the tool itself; and will automatically create the folder structure and name of the image files within those folders as illustrated in figure 1 (Symantec Corporation, 2004).

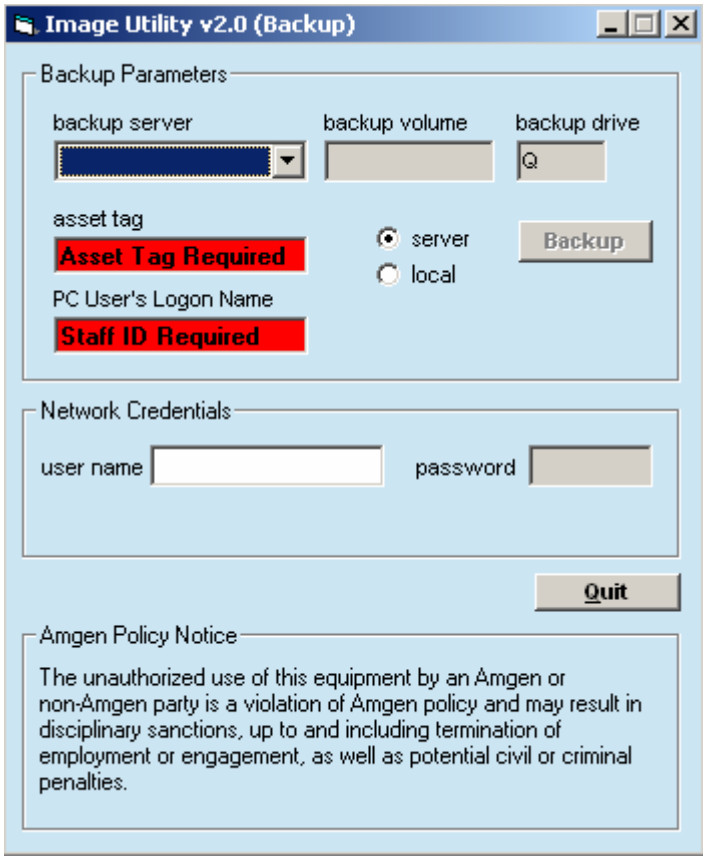

Figure 1 Norton Ghost Image Utility GUI (Symantec Corporation, 2004).

For applying a hard drive imaging tool to E-Discovery, the problem still exists of how to gain access to the data after it has been captured. Norton Ghost provides a unique tool in the Ghost Explorer which will allow an end user to navigate through the image file much like navigating in the Windows Explorer which is a tool that most end users are familiar with in getting to data on their own machines. The tool also allows for copying files out of the image

file by simply selecting the file and dragging it out of the Ghost Explorer interface to the desktop of the end user's machine see figure 2. While Ghost Explorer will also allow for modification of the image file, it is important to note at this point that the image files should ideally be stored in a controlled environment such as on a server with read only permissions such that no accidental overwrite or modification of the image file is possible. Alternatives include making a copy of the image files to another volume such that the original is not at risk (Burke, 2007).

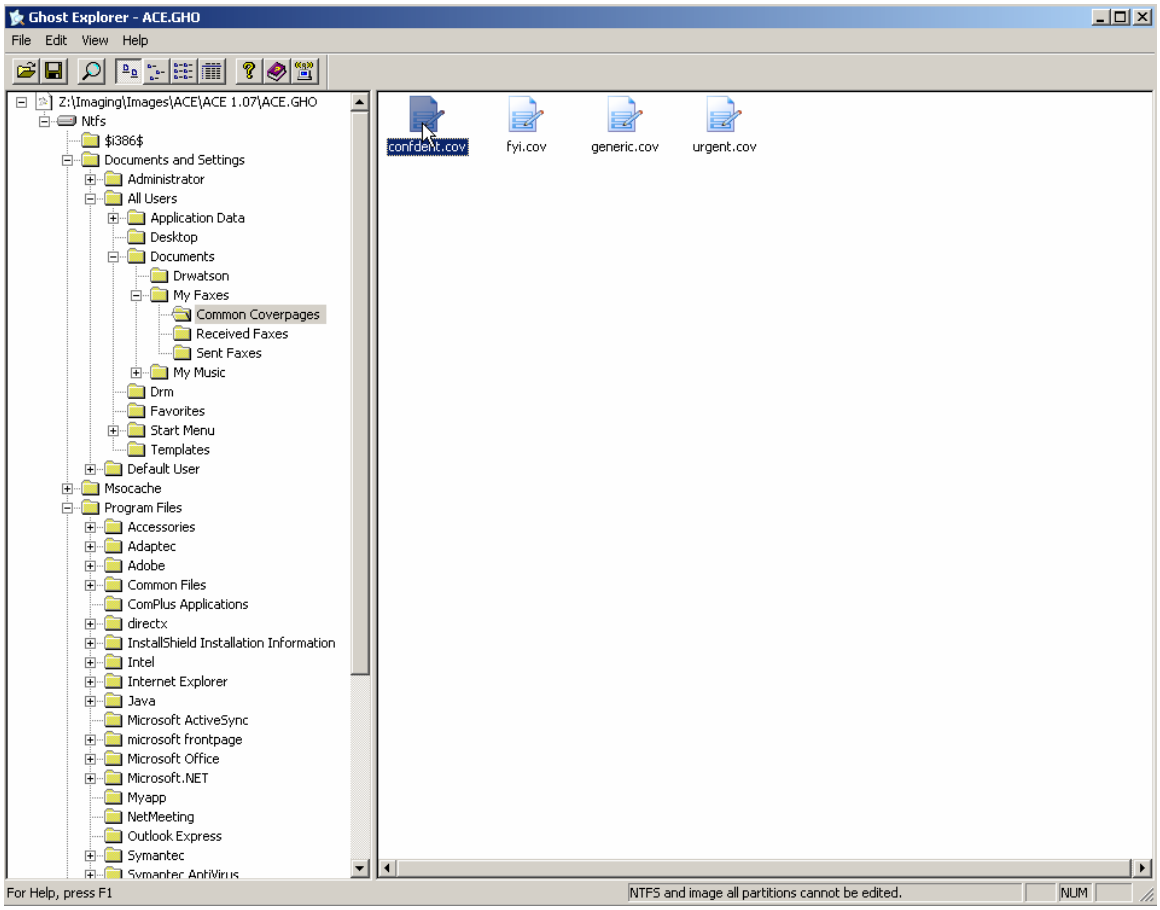

Figure 2 Ghost Explorer GUI (Symantec Corporation, 2004).

The importance of a tool that maintained the state information for the hard drive snapshot was imperative to the legal professionals as a requirement and for just cause. When a file such as a Microsoft Word document is opened, saved, modified, or changed in any way, specific data

referred to a metadata is captured within the file properties. Metadata is a term that refers to data about data with the most common metadata on a Windows system being the MAC times. MAC is an acronym for Modified, Accessed, and Created and is the metadata that is stamped into the file properties that may be accessed by right-clicking a file and getting properties on that file. For many files, this data may include the author's name, date the file was created on the system; last time the file was modified, when the file was last opened and viewed; and if supported, the system name the file was created on. In Windows systems that use the File Allocation Table [FAT] file format, the system time stamps are derived from the local system clock on the system which can pose an integrity problem for a system where the clock battery may have expired, or the system time experiences some form of drift over time. The NTFS file system however; stores its MAC times in Coordinated Universal Time [UTC] which is analogous to Greenwich Mean Time [GMT] and often, NTFS systems will update their system clocks by performing a routine time synchronization with a domain controller used for authenticating the system to the network resources (Carvey, 2007).

Metadata contained in Microsoft Word documents has been an issue for some time due to a technology that enables these documents to be compound documents linked to other documents and containing information about the file not readily visible to the end user. This technology called Object Linking and Embedding [OLE] was developed by Microsoft to allow the many different applications within the Microsoft Office Suite of products to interact with one another; call data from one another; import data from one another; and link the applications together such that Office could effectively be viewed as a suite of modules with specific functionality that is enabled to work together as a cohesive whole through the Office suite. Such metadata that might be stored within a Word document would be not only the past revision, but the last ten revisions

and last ten authors that edited a file posing an information disclosure risk for many people and organizations (Carvey, 2007).

Documents such as Portable Document Format [PDF] files can also contain metadata such as information about the application that created the file and even the type of system the file was created on such as an Apple Macintosh system versus a Windows based system (Carvey, 2007).

Francia & Clinton (2005) cite in their journal publication “Computer Forensics Laboratory and Tools”; “it is always prudent to avoid working directly on the evidence” and that “the need for excellent disk imaging process and tools is paramount” (p. 147). Considering the issue with file metadata and the fact that simply opening a file can alter this metadata; the selection of a tool that can capture the entire state of hard drive data yet allow that data to be accessed and copied out of the image file is paramount to maintaining the integrity of the original data collection should that original snapshot file come into question as to its integrity and efficacy such that the image snapshot file itself becomes evidence that is discoverable under certain challenges.

In evaluation of the software tools and the objective of e-compliance, it becomes clear that compliance with E-Discovery is not only a legal endeavor, but a technical endeavor as well. Close formalized relationships must be established between IT professionals and Law professionals to establish a clear understanding of the problems on both sides of the equation, and to assure that the tools selected meet the primary business objective for the legal professional in assuring E-Discovery compliance (Grasser & Haeusermann, 2007).

Chapter 6

Proposed Architecture Model for Data Collection Process

When collecting data from personal workstation computers and laptops, many stakeholders may become obsessed with the objective of getting that data however; how this is accomplished is as important as collecting the data itself. The process surrounding the activities in handling data in and of it self is a discoverable item and all of the practices, forms, documents, and tools used in the collection process may be evidence in a civil case. This is where proper information systems forensic practices and methods become most important. When a request for discovery of data is issued, despite the pressure from legal professionals and business management, it is advisable not to touch the computer system without following a proper forensic process that includes documenting everything that happens with the system; establishment of chain of custody for the computer system; storage of the equipment in secure location; and a proper secured work environment for the analyst to work in (Burke, 2007).

At the beginning of the process, a determination and risk assessment will be made regarding a legal action, suit, or potential for litigation. Based upon this assessment and determination, the legal council for the business or an area human resources representative may determine that data surrounding a particular system, or in most cases, and individual should be preserved for collection. This is referred to as a legal hold where the legal hold order suspends all data retention policy and activity that could result in modification or deletion of the data surrounding a computer system (Gasser & Haeusermann, 2007). This hold order can be issued via an electronic system such as a work order system, or it may be communicated via e-mail, and in the most rudimentary situation, a paper document ordering the system's preservation for collection will suffice. The common thread with all of these avenues is that there is a

documented method that records the action at the very beginning of the sequence of events. Verbal requests should not be used unless they are backed up by documentation as the documentation itself is evidence and may serve to protect the organization should the manner in handling the computer come into question.

An asset management system for tracking the asset numbers and / or serial numbers of computer systems assigned to individual end users is an essential component to enabling the business to identify what assets were assigned to the end user and ideally where that user was located within the enterprise such that the unit may be reclaimed by IT desktop personnel. If it cannot be found, it cannot be reclaimed. In smaller enterprises, this may not be as large an issue however; even in smaller enterprises and businesses it is a good practice to track the items in a desktop database systems such as Microsoft Access, Filemaker Pro, or even a Microsoft Excel Spreadsheet (Weaver, 2007).

Steven Hill (2006) cites in his article for Network Computing titled “Policy Workbook: E-Discovery” that “one of the dangers of e-discovery data collection revolves around the issue of spoliation, legalese for the destruction or alteration of evidence or the failure to preserve evidence in pending or reasonably foreseeable litigation” (p. 2). Considering this risk, the best practice is for IT personnel within an organization to leverage a standard forensic practice for handing evidence by reclaiming any desktop or laptop equipment assigned to an end user and placement of that equipment into a controlled quarantine for a specific period of time where it is tagged; secured; free of electromagnetic fields, free of static and dust; and accessible by an analyst in a functional environment for analysis (Yeager, 2006).

Quarantine of systems for a specific period of time before the drives are erased can not only aid in E-Discovery compliance but also provide a medium for protecting the organization's intellectual property especially if the employee works with confidential and proprietary information, trade secrets, or other information important to the business where that information in and of itself is considered an asset. Thus, if the loss of such information poses a risk to theft, damage, financial loss, liability, or compliance with regulatory laws; quarantine of equipment offers a medium for preserving this information beyond E-Discovery compliance (Weaver, 2007).

Once the evidence has been identified, seized and placed into a controlled quarantine, the forensic best practices come into play. Establishing chain of custody documentation; photos of the evidence to record any damage; sealing the computer case; determining how many people and what their individual roles are in relation to access to the controlled environment and quarantine location (Burke, 2007); and recording the unit in any necessary asset databases with the disposition are essential not only in ensuring that the units can be available for a data collection, but also that they are available for data cleansing once the quarantine period has expired for the computer workstation or laptop. Grance & Stevens (2004) in their guide "Security Considerations in the Information System Development Life Cycle" distributed through NIST, refer to this cleansing process as "*Media Sanitation*" where "deletion of any residual magnetic or electrical representation of data is, deleted, erased, or written over" (p. 32). This process ensures that no data can be reconstructed or retrieved at a later date minimizing risk of sensitive or proprietary information from accidentally being leaked out of the organization as well as minimizing risk associated with that data's continued existence in a non-controlled location. This same process of Sanitization is also essential for any legacy equipment that might

be donated or disposed of where the computer ultimately leaves the organization's property and falls into third party hands.

Should a legal hold and collection request be received for a particular user or system; that system is then pulled from quarantine, associated documents or databases for check-out and check-in are logged; and the unit is prepared for a data collection. As it has been established that "relevant data must be kept meticulously in tact and include the metadata that verifies it's authenticity and accuracy" (Hill, 2006, p. 2); the best method for assuring this is to use a hard drive snapshot tool that can capture the entire contents and state of the drive in its entirety. This is referred to under the Federal Rules of Civil Procedure as *Best Evidence* which allows for a forensic duplicate of the drive as admissible in lieu of the original where the original is not available or would pose some hardship in producing it to the court (Steel, 2006). Chad Steel (2006) further illustrates that "Creating a forensic image of a hard disk is one of the most common forensic techniques used" (p. 194) This is due in part to the burden and cost to remove hard drives from the computer workstation requiring a replacement to bring the unit back into serviceability; and a greater consideration is in the fact that a hard disk is a mechanical device which due to it's mechanical nature may be prone to a failure or crash resulting in loss of the evidence (Wires & Feeley, 2007). "A hard disk crash used to mean that the heads literally crashed into the platter, destroying both the head and the platter itself though, now the term crash is used to denote a less fatal failure as well" (Steel, 2006, p. 52). This is an important consideration as determination of where to send our forensic duplicate also plays a factor. In an ideal situation, it is best to send the hard disk forensic duplicate or snapshot to a file server with the appropriate security permissions to protect the data. As most servers and network appliances use RAID which stands for Redundant Array of Inexpensive Disks, to store information, the

failure of one disk does not result in the loss of data as a RAID drive array can rebuild the contents of the failed drive once it is replaced (Microsoft Training and Certification, 1999). Also servers in many large enterprises support tape backup offering yet more fault tolerance. This ensures "data durability to protect the data from accidental or malicious destruction" (Wires & Feeley, 2007, p. 214). The alternatives for storing the image snapshot include using an external large capacity hard drive, sending the data to DVD-R or even to a flash media drive if space permits (Steel, 2006). However; none of these options offer the fault tolerance or security of a network server.

As Norton Ghost will literally take a snapshot the entire hard drive and its contents, this will create an immutable snapshot that is free of the risk of erroneous file-system actions (Wires & Feeley, 2007). As the operating system itself may contain critical evidence stored within its registry hives, the ability to capture this information along with any documents of relevance may prove valuable in an E-Discovery case. The Windows Registry Hives consist of five distinct root folders which play a critical role in the function of the computer system:

- "HKEY_USERS hive contains all of the actively loaded user profiles for that system" (Carvey, 2007, p. 128).
- "HKEY_CURRENT_USER is the active, loaded user profile for the currently logged-on user" (Carvey, 2007, p. 128).
- "The HKEY_LOCAL_MACHINE hive contains a vast array of configuration information for the system, including hardware settings and software settings" (Carvey, 2007, p. 128).
- "The HKEY_CURRENT_CONFIG hive contains the hardware profile the system uses at startup" (Carvey, 2007, p. 128).

- “HKEY_CLASSES_ROOT hive contains the configuration information relating to which application is used to open various files on the system” (Carvey, 2007, p. 128).

Consider the information stored within the Windows Registry Hives, this data can provide critical information about a case including installation dates for applications; how many people and who they were that had access to the local machine; and other information that may provide context to the file metadata contained within an electronic document.

The application of Unified Modeling Language [UML] diagrams illustrates the hard drive collection process in terms of the Use-Case Scenario; State Diagram; and Sequence Diagram. Use-Case describes the benefit in how the system is used by the end users who are referred to as *Actors* and illustrates in a simple depiction of how the user interacts with the system, process, or combination thereof. State Diagrams capture the state an object can have during the life cycle of the process or work flow. Sequence Diagrams illustrate the collaboration between a number of objects or systems in terms of messages or communication between those systems. The application of UML provides a standardized method for modeling visualizations, specifications, construction, documentation and communication of system designs in a format that may be more easily understood by multiple stakeholders (Erikson, Penker, Lyons and Fado, 2004).

The following illustrates the Use-Case scenario for the computer data collections.

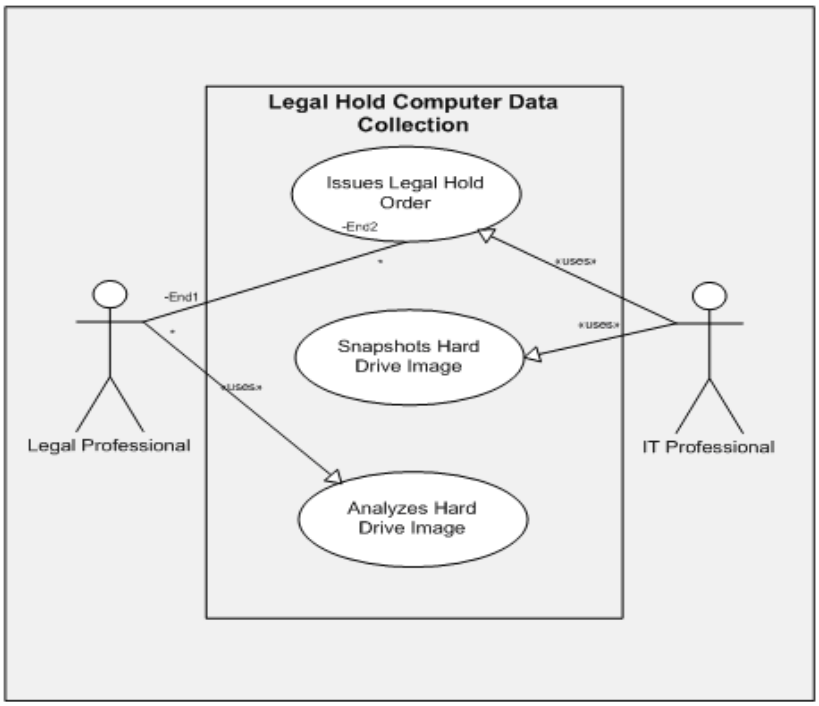

Figure 3 Use-Case Scenario for Legal Hold Computer Data Collection.

Legal Hold- Computer Data Collection

1. **Iteration:** v 1.0

2. **Summary Objective:** When the legal professional issues a legal hold order, specific data must be preserved and all destruction policies specified under the Data Retention Policy must be suspended. IT personnel collect the data so that it may be analyzed and reviewed by the legal council.

3. **Initiation Trigger:** Litigation in a Civil Suit has been initiated against the organization.

4. **Flow:** Legal issues a hold order.
    a) Designated IT personnel receive the hold order.
    b) IT retrieves the computer from quarantine.
    c) IT sets up the computer and boots to a PE bootable drive.
    d) IT runs the Ghost Imaging Utility to snapshot and image of the hard drive.
    e) IT returns the computer to quarantine until expiration of the quarantine period.
    f) IT transfers the image snapshot to a controlled storage volume.
    g) IT updates chain of custody forms and databases.

5. **Alternate Flow:** Computer quarantine period has expired or no individual computer asset was assigned to user ending the collection process.

6. **Business Rules / Supplemental Requirements:** Data is only collected from computer equipment that was assigned to an individual user.
    a) The IT Professional account has permission to access the storage volume.

7. **Finish:** The hard drive data is retained.
    a) Legal Professional analyzes the image file for documents and information related to the litigation using Ghost Explorer.
    b) IT erases the computer hard drive at the end of the quarantine period.

The flow of information in terms of the computer systems communication with one another is illustrated in the Sequence Diagram in Figure 4.

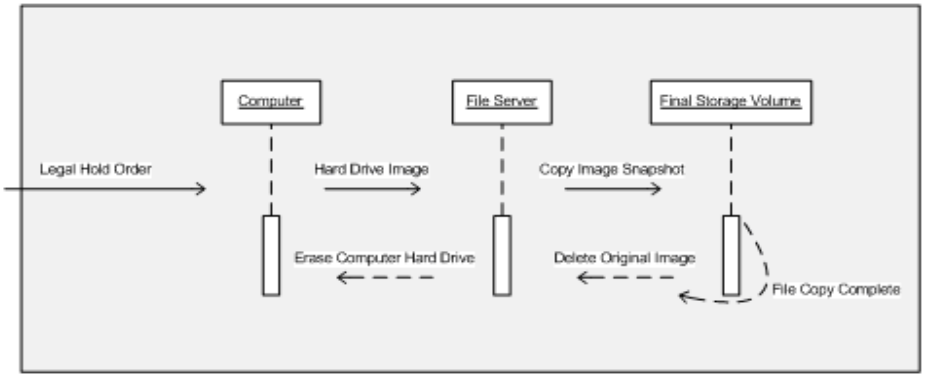

Figure 4 Sequence Diagram for Computer Data Collections.

The State of the computer and the data contained on the hard drive is illustrated in Figure 5:

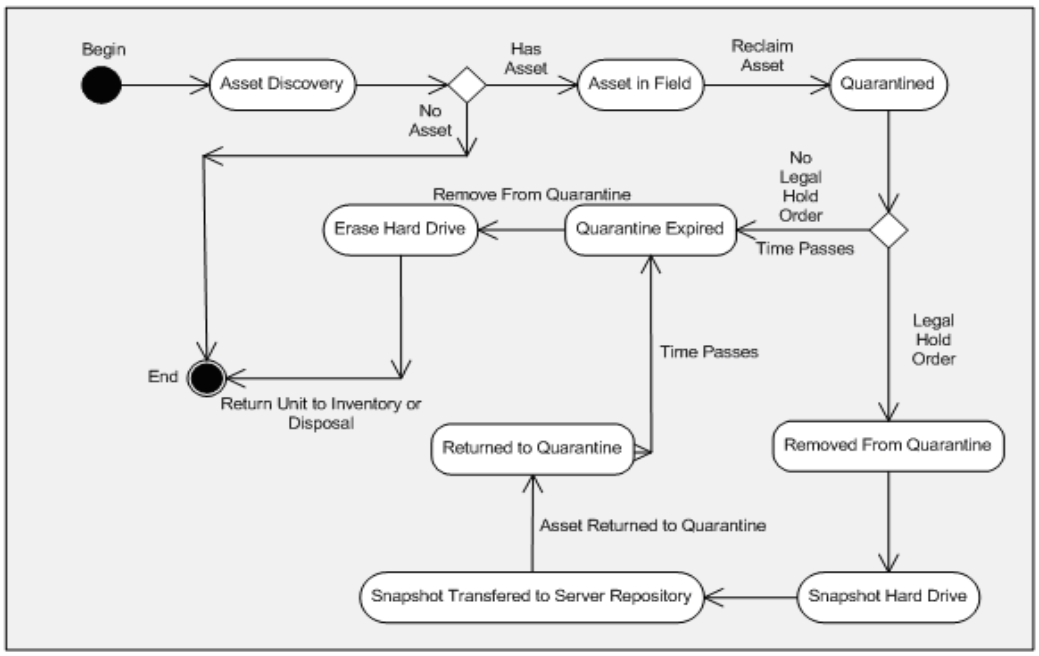

Figure 5 State Diagram for Computer Data Collections.

In the final phases of the Sequence Diagram erasing the hard disk is specified. This aligns with the establishment of a data retention policy. Considering the discoverable nature of electronic data, maintaining extensive volumes of erroneous data over long periods of time can create risk and vulnerability by the nature of such data's existence in the enterprise. The Federal Rules of Civil Procedure Rule 26 2(B) provides for an exception to discovery for "electronically stored information from sources that are identified as not reasonably accessible because of undue burden or cost" and Rule 37 cites that "a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system" (LexisNexis Federal Rules of Civil Procedure, 2007). Council should be prepared to defend clearly any policies surrounding data retention on behalf of their clients however; under these rules, undue hardship can be argued in terms of the implications of long term storage costs associated with large volumes of electronic data. In consulting with a legal professional in the Fortune 500 Pharmaceutical company for our

project, the erasure policy for desktop computer workstations and laptops was set at thirty days following a person leaving the company as most litigation will occur within this thirty day period if it is going to happen at all. This also ensures that multiple data sets of same data types do not exist in relation to a legal hold such that the information remains in one central location under the collection process. Mary Pat Gallagher (2007) cites in the New Jersey Law Journal publication "No computer tampering proved in test case of e-discovery rules" that "If you're really worried about electronic discovery, throw it in the garbage" (p. 2). While Gallagher is not endorsing willfully destroying data associated with a legal hold order, she is illustrating the point that maintaining volumes of legacy electronic data for long periods of time does pose a risk for an organization and should be deleted unless otherwise protected under regulatory compliance or preservation of intellectual property for operation of the business (Gallagher, 2007).

Browning Marean (2007) cites in the journal publication "E-Discovery looks like risky business" that "To my knowledge, no law school teaches a course in project management" (p. 2). When it comes to dealing with electronic data discovery, leveraging good project management skills such as establishing a detailed work breakdown structure (WBS) can provide great benefit to the process in defining how tasks will be allocated, stakeholders involved, and defining a work flow such that defining chain of custody can be more easily accomplished.

Kathy Schwalbe (2006) cites in the book "Information Technology Project Management Fourth Edition" that "Project Scope Management includes the processes involved in defining and controlling what is or is not included in a project" (p. 179). The Work Breakdown Structure (WBS) is an element of Project Scope Management where the WBS "involves subdividing the major project deliverables into smaller, more manageable components" (Schwalbe, 2006, p. 175).

A simple tabular form WBS for a hard drive data collection process as Schwalbe (2006) would present it:

Legal Hold Hard Drive Data Collections WBS

1. Concept

Identify Risk

Define Legal Hold Notification Process

Identify Target Assets

Define Collection Tool Requirements

Identify Stakeholders and Participants

Identify Project Champion from Senior Level Management

2. Process Design

Define Physical Collection Procedure

Define Quarantine Period

Establish Secure Quarantine Area

Define asset tracking method or how existing asset tracking method will be leveraged.

Define storage volumes and permissions structure for those network servers that will contain the volume.

Define software collection toolkit build.

Define chain of custody procedure for image handling and transfers between agents and locations.

Define Data Retention Policy for Hard Drive Erasure

3. Process Implementation & Rollout

Build External PE Bootable Kits

Train IT agents in handling physical evidence and collection procedures.

Train Legal Professionals in using Ghost Explorer tool for accessing data for analysis and recovery.

Define Legal Hold communication strategy and method

Begin Hard Drive Image Snapshot Collections

There are a number of methods for devising and documenting a Work Breakdown Structure including flow charts and software applications such as Microsoft Project however; the tabular form provides the simplest approach and the data captured in this structure may then be applies to a more complex model or software tool.

During each step and phase of the collection process, it is essential that the personnel that handle the data, or the components that contain the data, document their actions and activities. Transfer of the data is a custody issue handled under chain of custody procedures however; there are other important items that should be documented in a evidence sheet or work log such that situations such as an unbootable drive; sector damage to the hard disk; or any other activity that may require altering the state of the hard drive such as repairing the damaged sectors with a tool; or any other diagnostic procedure should be logged and recorded as this activity may raise question to the efficacy of the data collected unless these actions are recorded somewhere (Burke, 2007). Christy Burke (2007) cites “The prospect of filling out endless log forms is enough to put anyone to sleep but a string of recent judicial sanctions over chain of custody for electronic evidence has made the dry issue a hot topic and one that can make or break your case” (p. 1). This can be extremely important for example, if the hard drive requires professional services to reclaim the data or the drive itself is requested by the legal department as evidence. If

this scenario occurs, often commercial carriers are sufficient to transport the evidence but in rare situations a carrier that offers greater security will be required (Burke, 2007). If evidence is shipped by a carrier, the shipping forms become part of the chain of custody records as it will show the date the item was shipped to another location and the name of the carrier that handled it.

When analyzing data, the prospect of digging through thousands of electronic files can be a daunting task. Unlike a flat file document storage system where file cabinets and paper records are kept, often many users ironically are not as organized in their storage of files on their personal computer. Microsoft provides a folder titled *My Documents* for storing files however; when one considers the concept of a picture is worth a thousand words, perhaps Microsoft should have used an icon for a filing cabinet rather than a file folder. McGovern, Ambler, Stevens, Linn, Sharan, and Jo (2004) describe the classification of data relating to security classifications as "unrestricted, research and development, operations, partner, governmental information, and national security" (p. 242). Considering the overwhelming amount of electronic data that may be generated by an individual user at a company, consideration should also be given to the creation of a data classification system for that data.

Butler, Rogers, Ferratt, Miles, Fuller, Hurley et al. (2007) state that "data classification allows an organization to clearly define the importance of information types to the organization and based on those classifications, an organization can determine an appropriate level of protection for each information type" (p. 49). A data classification method can be highly valuable in relation to E-Discovery requests as pursuant to Rule 26 (B) of the Federal Rules of Civil Procedure, "If information is produced in discovery that is subject to a claim of privilege or of protection as trial-preparation material, the party making the claim may notify any party that

received the information of the claim and the basis for it.. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has and may not use or disclose the information until the claim is resolved" (LexisNexis Federal Rules of Civil Procedure, 2007). As it is a fair expectation that legal council will be expected to justify and clearly illustrate such classifications or policies, the adoption of a data classification method can aid in this justification as evidence in and of itself. Such classification may take the form of data type levels of criticality to the business such as Level 1 Data where the data is considered normal information, low relevancy to the business, etc; up to Level 5 Data which may be the most classified data in the company such as the formula for a key product that is the basis of the company's intellectual property. However the organization decides to classify its data whether it is Confidential, Secret, Top Secret; Level 1, Level 2, Level 3; Class A, Class B, Class C, etc; will be determinate upon the method that bests align with the business or organization. Ultimately, the classification model should be easy and clear enough for people to understand and use such that it is easy enough for a third party such as a court or jury to understand.

In establishing and architecting a model for E-Discovery collection of electronic data stored on personal computer workstations and laptops, these key principles will go a long way to establishing a process that fulfills the *good faith* effort prescribed in the Federal Rules of Civil Procedure.

Chapter 7

Analysis of the Data Collection Project Results

Eoghan Casey (2006) cites in the ACM Publication "Next-generation Cyber Forensics: Investigating Sophisticated Security Breaches" that "a successful digital investigation is heavily dependent on the logging and backup systems and organization has in place, and how quickly sources of evidence are located and preserved" (p. 50). Casey (2006) goes on further to illustrate "all of this collection is performed in a forensically sound manner to ensure that complete and accurate copies are obtained and the authenticity and of the evidence is documented for future reference" (p. 51). Casey's statements support the thesis behind this project.

To test the thesis and apply the architecture solution in a real world environment, this project was executed in a Fortune 500 Pharmaceutical Company. The agreement with this company by non-disclosure agreement shall avoid using the company's name within the documented report and shall refer to the company as *A Fortune 500 Pharmaceutical Company*. No names of individual participants or proprietary information owned by this company may be disclosed in this document.

The project team launched in October of 2007 with the objective of establishing a collection method for data contained on individual computer workstations and laptop systems as illustrated in Chapter 6. The core team was comprised of a manager from the records and compliance office within the Law department; a member of the desktop architecture organization with specialization in the hard drive imaging, a member of the Information Security [Infosec] organization, and this author with expertise in vendor management, Infosec, imaging technologies, and management of the local desktop environment.

In its initial state, prior to the initiation of this project, the collection method had several key problems that had to be overcome. The chain of custody process illustrated several gaps where formal notification and record keeping was handled solely by the Infosec representative and the records retention department however; there was no medium of activity tracking for peripheral operations that handled the evidence. Communications to these peripheral areas lacked consistency where in some cases a simple e-mail would be sent or forwarded, and in other cases a phone call was received. The other major issue was the tool being used in the Microsoft User State Migration Tool 3.0 which failed to capture the entire state of the machine focusing only on the documents collection aspect. To solve these two problems, the team had to agree on the importance of the maintaining the user state such that an agreed upon tool could be implemented. One consideration was that due to the changes in Rule 34 of the Federal Rules of Civil Procedure, discussion and agreement on the form the electronic data will be produced is specified by the requesting party (Shelton, 2006) thus, until this discussion occurs, the owner of the electronic data has no idea what format will be requested and should maintain the state of the entire drive contents so that all data is available and retrievable. Following this, a procedure that surrounded the use case scenario for the tool selected for our project could be established closing the gap for the chain of custody and documentation areas of the process. Mary Pat Gallagher (2007) cites a case in her New Jersey Law Journal Publication "No computer tampering proved in test case of e-discovery rules" that plaintiffs in the test case challenged the defendant in their claim of copying the data, "how do we know?" (p. 2). In the case cited by Gallagher (2007) the judge ultimately ruled that the burden of proof that the data was deliberately thrown out was on the plaintiff, not the defendant however; as with standard electronic evidence procedures, the records of how the data was handled is evidence in itself and therefore lack of record keeping

could be used to demonstrate negligence in procedure or lack of good faith effort. This boils down to the risk that when digital evidence is not forth coming, court orders may be used to obtain the data as well as impounding of any extraction tools used in order to determine if proper protocols had been applied properly (Mercuri, 2005).

The results of these initial project meetings yielded that we needed to review and establish assurance that the quality and efficacy of the data within the company's asset tracking database system was as accurate as possible. This would be necessary for identifying if the target of a Legal Hold Order had a personally assigned personal computer or not. It was determined that only primary assigned assets where an individual computer was assigned to an individual end user would be subject to collection. All computer equipment designated as common use, general use, or some form of shared status would not be considered collectable as these units were regarded as simple tools and would pose an undue burden and hardship on the company to reclaim instrument controllers, training systems, and other common use terminals as this would impact the remaining users and business functions still dependent upon the computer and would result in significant cost to replace the units each time a person who touched a computer left the company.

A quarantine area and process had to be identified such that the area was protected from unauthorized personnel access to the area, and had some form of monitoring in place. The quarantine in the project was secured behind several layers of badge access controlled rooms where the access control logs could be audited for who accessed the area and at what time; and the entire area was monitored by a 24 x 7 Closed Circuit Television (CCTV) array of cameras which recorded digital footage of the quarantine area retained for ninety days placing the retention at sixty days past the quarantine period for auditing purposes.

The work order request system had to be modified to accommodate routing of work tickets such that the proper field technicians were notified in a common request medium to reclaim the asset and take it to the secure quarantine area. This also created a consistent searchable repository of records that began the process for how the evidence was handled at the moment the instruction for collecting the unit was initiated.

In using a hard drive snapshot tool such as Symantec's Ghost application where the tool captures the entire contents of the computer hard drive, storage of this high volume of data can be quite large depending on the size of the organization. In assessing the snapshots in this project, the average snapshot size was approximately seven gigabytes of data per hard drive image. This included the Windows operating system, Office 2003 Standard, Acrobat Reader, and all documents or additional applications loaded by the end user. In the first week following the collection procedure launch, the seven terabyte volume allocated for storing the hard drive images filled up completely requiring archival before additional transfers could be completed. To put this volume of information into perspective, Gregory Shelton (2006) describes the terabyte in the journal publication "Don't let the terabyte you: new e-discovery amendments to the federal rules of civil procedure" as "a unit of measurement for data storage capacity that is roughly equivalent to 50,000 trees made into paper and printed; it is 500 million typewritten pages of plain text; it is enough words that it would take every adult in America speaking at the same time five minutes to say them all" (p. 324). At seven terabytes per hard drive snapshot image, to fill up a seven terabyte NetApp Server equaled about 1000 hard drive images before the data had to be archived. This raises the argument that many enterprises may not be prepared for the storage requirements associated with E-Discovery collections depending upon their size and budgetary spending on server based storage.

For chain of custody record keeping, the project initially utilized a Word template form that accompanied the electronic image file. While this approach enabled documentation of the chain of custody procedure, the ability to track the chain of custody in a centralized electronic reference repository was problematic. To solve this problem, the Records Retention Department under the Law Department had an Oracle APEX database built to track the chain of custody information for data collection transfers. This afforded the entire North American enterprise to track the chain of custody in a Web accessible centralized information system that incorporate login authentication for security control, reporting, and historical data.

Once the collection method for existing data was in place and determined to be effective and successful, efficiency in future cases became the focus of the project. This led to the implementation of a data classification strategy which proposed organizing the data by data types and relevance such that the data could be more easily searched and discovered by legal professionals in the future should it become necessary. As a result, a folder structure was designed that subdivided data types into classifications such as budget information, time off requests, business reports, goals and objectives documents, governance documents, and project management documents. This folder structure was deployed through electronic software distribution to the entire general desktop computing domain via System Management Server [SMS] 2003 and placed in every staff member's My Documents folder.

While the storage folder structure has been made available to the enterprise, and the folder structure is viewed as implicit in itself; it has been argued with the global project team that the lack of an official policy supported by executive management regarding this storage structure as well as lack of active marketing for the use of the new folder structure may result in staff not

using the structure or deleting the folders simply because of a lack of awareness of their importance to finding documents at a later date.

In looking back at our survey results, our Fortune 500 Pharmaceutical Company is aware of the E-Discovery compliance issue; this enterprise has document management systems, centralized server based storage for end user data; has an information security function; has a number of data retention policies; reclaims desktop and laptop computer workstations when a person leaves the company; quarantines those computers for a thirty day period following the reclamation of the hardware; and has a desktop hard drive imaging application used for deploying standard build OS configurations; denoting that the enterprise had the core systems and technologies in existence that could be leveraged for E-Discovery hard drive data collections.

By applying standard Information Systems Forensic best practices and leveraging these existing systems within this enterprise, the Fortune 500 Pharmaceutical Company was able to successfully implement a data collection method based upon the proposed architecture in chapter five leveraging these internal resources at a minimum of cost to the enterprise with most of the cost impact surrounding restructuring some processes and technical staffing to handle the collection process itself.

Chapter 8

Summary

The thesis for this project presents that leveraging traditional data forensic analysis best practices for data classification and collection procedures can solve the E-Discovery compliance problem. Distributed computing has become a fact of life in the modern business enterprise resulting in data being distributed across many computer systems throughout the network

domain. Because of this distributed nature for large amounts of electronic information, such information is routinely modified, overwritten, updated, and deleted as a part of normal business practice (Shelton, 2006). Even though the Federal Rules of Civil Procedures rule 26 provides for challenges where discovery would impose undue burden and cost to an organization, this is not a blanket defense thus; it is essential that an organization also fulfill the provisions of rule 37(f) which states that a court cannot impose sanctions where a *good faith* effort to comply with an electronic discovery request has been made (Hill, 2006).

The survey for this project revealed that a number of enterprises ranging from small, medium, and large have the baseline capabilities and tools for collection of electronic data from workstation computers distributed throughout the organization. For those that do not have these baseline capabilities, the proposed architecture in chapter 6 can aid in establishing a program for collecting data from computer workstations and laptops with a minimal expense and effort. The key points to understand are the information systems forensic analysis best practices for how electronic data is handled and where those practices serve to strengthen a case for computer based investigations in the criminal court system such that they may also be leveraged to build credibility in the data collected for civil court electronic discovery. Leveraging a hard drive snapshot software tool is the simplest method for collecting not only the data stored on the local drive, but the metadata and context that surrounds it (Carvey, 2007).

Considering that critical records are increasingly stored electronically, more so now than ever before, and this electronic format can make it very easy for such information to be modified or destroyed with relative ease; when it comes time for that data to be collected for analysis in E-Discovery it is imperative that the data be managed in a proper manner to ensure the trustworthiness of the information disclosed (Zhu and Hsu, 2005). Establishing an E-Discovery

policy and process can greatly minimize the risk of sanctions being imposed as a result of perception of illegal destruction of evidence by a court (Preimesberger, 2007) however; as many cases may never go to a trial including those that result in out of court settlements, dropping the case, or a suit never being filed to begin with (Mercuri, 2005); expenditure of excessive amounts of corporate funding for a *what if* scenario may not be in the organization's best interests financially especially where the cost to covert electronic documents can range five to twenty cents per page, and to convert hundreds of thousands or even millions of documents could result in cost of $50,000 and higher (Sherman and Steidl, 2007). For this *just in case* scenario; taking a simple snapshot of the computer hard drive and documenting the handling of this data with chain of custody procedures will provide the organization of relative assurance that the *good faith* attempt to capture and retain electronic data has been fulfilled.

Conclusion

Litigation is quickly becoming a cost of doing business where a large enterprise may find itself dealing with several or even hundreds of lawsuits per year and although local jurisdictions may impose their own rules for E-Discovery, the Federal Rules of Civil Procedure is often what they will pattern their process after if for no other reason than simplicity and standardization in the process (Hill, 2006). Given this risk to business enterprise, organizations must care about the regulations and compliance issues that affect them and arguably they should want to care (Butler, Rogers, Ferratt, Miles, Fuller, Hurley, et al., 2007).

Organizations have struggled for years to manage excessive volumes of electronic information and data while at the same time, academic professionals, business professionals, software vendors, and industry experts have strived to create methods, tools, and practices to aid in this objective. With the advent of E-Discovery, a whole new industry is beginning to evolve

to offer a solution for the E-Discovery problem however; leveraging the tools and practices that already exist can save an organization significant expense and effort by leveraging the information and tools that already exist and can aid in solving this problem for the business. In the end, it is a matter of getting organized with managing electronic data more than buying a solution.

Table of Figures:

References:

Adelstein, F. (2006) Next-generation Cyber Forensics: Live Forensics: Diagnosing Your System Without Killing It First. Communications of the ACM, Volume 49 Issue 2. [65] Retrieved September 17, 2007 from http://delivery.acm.org.dml.regis.edu/10.1145/1120000/1113070/p63-adelstein.pdf?key1=1113070&key2=5215700911&coll=ACM&dl=ACM&CFID=30104998&CFTOKEN=11098819

Baron, J. R., Thompson, P. (2007). Legal Information Retrieval: The search problem posed by large heterogeneous data sets in litigation: possible future approached to research. Proceedings of the 11th international conference on Artificial intelligence and law ICAIL '07. ACM Press. [141] Retrieved September 23, 2007 from http://delivery.acm.org.dml.regis.edu/10.1145/1280000/1276344/p141-baron.pdf?key1=1276344&key2=9644700911&coll=ACM&dl=ACM&CFID=30104998&CFTOKEN=11098819

Becerra-Fernandez, I., Gonzalez, A., Sabherwal, R. (2004) Knowledge Management: Challenges, Solutions, and Technologies. Pearson Prentice Hall. Pearson Education Inc. [213]

Burke, C. (2007) Examining e-discovery chain of custody. New Jersey Law Journal. LegalTrac. Gale. BCR Regis University. [1-3] Retrieved on January 2, 2008 from

http://find.galegroup.com.dml.regis.edu/itx/retrieve.do?contentSet=IAC-Documents&resultListType=RESULT_LIST&qrySerId=Locale%28en%2C%2C%29%3AFQE%3D%28ke%2CNone%2C11%29E-Discovery%24&sgHitCountType=None&inPS=true&sort=DateDescend&searchType=AdvancedSearchForm&tabID=T002&prodId=LT&searchId=R1&currentPosition=3&userGroupName=regis&docId=A170240519&docType=IAC

Butler, C., CISSP., Rogers, R., CISSP., Ferratt, M., JNCIS-FWV., Miles, G., CISSP., Fuller, E., Hurley, C., IAM/IEM., et al. (2007) IT Security Interviews Exposed. Wiley Publishing Inc. [49, 54-55, 61]

Carvey, H. (2007) Windows Forensic Analysis Incident Response and Cybercrime Investigation Secrets. Syngress Publishing, Inc. [128, 230, 232, 238, 263]

Casey, E. (2006) Next-generation Cyber Forensics: Investigating Sophisticated Security Breaches. Communications of the ACM, Volume 49 Issue 2. [50-51] Retrieved September 17, 2007 from http://delivery.acm.org.dml.regis.edu/10.1145/1120000/1113068/p48-casey.pdf?key1=1113068&key2=7025700911&coll=ACM&dl=ACM&CFID=30104998&CFTOKEN=11098819

CommVault. (2007) CommVault Solutions – Legal Discovery. CommVault. Retrieved June 18, 2007 from

http://www.commvault.com/solutions/legaldisc/index.asp

Cornell Law School. (2007) Federal Rules of Civil Procedure Contents and Context. LII / Legal Information Institute. [Rule 26, Rule 34], Retrieved June 20, 2007 from http://www.law.cornell.edu/rules/frcp/

Eriksson, H-E., Penker, M., Lyons, B., Fado, D. (2003) UML 2 Toolkit. New York: John Wiley & Sons. [1, 29-30, 58-63, 145-149]

Francia, G. A., Clinton, K. (2005) Computer Forensics Laboratory and Tools. Journal of Computing Sciences in Colleges, Volume 20 Issue 6. [143-147] Retrieved September 17, 2007 from http://delivery.acm.org.dml.regis.edu/10.1145/1070000/1060428/p143-francia.pdf?key1=1060428&key2=9005700911&coll=ACM&dl=ACM&CFID=30104998&CFTOKEN=11098819

Friedman, L. M. (2007) A History of American Law Third Edition. Touchstone A Division of Simon & Schuster, Inc. [516-537]

Gallagher, M. (2007) No computer tampering proved in test case of e-discovery rules.(New Jersey). New Jersey Law Journal. LegalTrac. Gale. BCR Regis University. [1-2] Retrieved on January 2, 2008 from

http://find.galegroup.com.dml.regis.edu/itx/retrieve.do?contentSet=IAC-Documents&resultListType=RESULT_LIST&qrySerId=Locale%28en%2C%2C%29%3AFQE%3D%28ke%2CNone%2C11%29E-Discovery%24&sgHitCountType=None&inPS=true&sort=DateDescend&searchType=AdvancedSearchForm&tabID=T002&prodId=LT&searchId=R1&currentPosition=21&userGroupName=regis&docId=A158947863&docType=IAC

Gasser, U., Haeusermann, D. (2007) E-Compliance: Towards a Roadmap for Effective Risk Management. The Berkman Center for Internet & Society at Harvard Law School. Research Publication No. 2007-3. [4, 9, 17, 19] Retrieved July 17, 2007 from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=971848

Gottschalk, L., Liu, J., Dathan, B., Fitzgerald, S., Stein, M. (2005) Computer Forensics Programs in Higher Education: A Preliminary Study. ACM SIGCSE Bulletin, Proceedings of the 36th SIG CSE technical symposium on Computer science education SIG CSE '05, Volume 37 Issue 1. ACM Press. [147] Retrieved September 17, 2007 from http://delivery.acm.org.dml.regis.edu/10.1145/1050000/1047403/p147-gottschalk.pdf?key1=1047403&key2=9454700911&coll=ACM&dl=ACM&CFID=30104998&CFTOKEN=11098819

Grance, T., Hash J., Stevens M. (June 2004) Security Considerations in the

Information System Development Life Cycle. NIST. Technology Administration U.S. Department of Commerce. [5, 31-33] Retrieved March 23, 2005 from http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf

Hartwig, R. PhD., Hudgins IV Esq., J. M. "Skip"., McAuliffe, T., Woollams, R. (2007) U.S. Tort System 2007: How rough is the ride ahead? American Tort Reform Association. [4] Retrieved July 17, 2007 from http://www.aigamericanhome.com/americanhome/public/ahafiledownload/0,1841,1164,00.pdf

Hill, S. (2006) Policy Workbook: E-Discovery. Network Computing. CMP Media LLC. [37-39] Retrieved on January 2, 2008 from http://www.lexisnexis.com.dml.regis.edu/us/lnacademic/results/docview/docview.do?risb=21_T2773060824&format=GNBFI&sort=RELEVANCE&startDocNo=1&resultsUrlKey=29_T2773060827&cisb=22_T2773060826&treeMax=true&treeWidth=0&csi=155287&docNo=14

Jones, K. J., Bejtilich, R., Rose, C. W. (2006) Real Digital Forensics Computer Security and Incident Response. [163-169] Pearson Education Inc.

Lagerweij, B. (2000-2008) Bart's Preinstalled Environment (BartPE) bootable live windows CD/DVD. NU2 Website. Retrieved on February 24, 2008 from http://www.nu2.nu/pebuilder/

Lang, J. P., and Baffa, J. (2007) Electronic Discovery: An Overview And Practical Pointers. Bates & Carey LLP. Retrieved September 23, 2007 from http://www.batescarey.com/newsandarticles/electronicdiscovery.asp

Lexis Nexis® (2007) Federal Rules of Civil Procedure. LexisNexis, a division of Reed Elsevier Inc. Retrieved April 30, 2006 from http://www.lexisnexis.com/lawschool/learning/reference/pdf/2006/LA11909-0_FRCP.pdf

Marean, B. (2007) E-discovery looks like risky business. New Jersey Law Journal. LegalTrac. Gale. BCR Regis University. [1-2] Retrieved on 2 January 2, 2008 from http://find.galegroup.com.dml.regis.edu/itx/retrieve.do?contentSet=IAC-Documents&resultListType=RESULT_LIST&qrySerId=Locale%28en%2C%2C%29%3AFQE%3D%28ke%2CNone%2C11%29E-Discovery%24&sgHitCountType=None&inPS=true&sort=DateDescend&searchType=AdvancedSearchForm&tabID=T002&prodId=LT&searchId=R1&currentPosition=1&userGroupName=regis&docId=A170459778&docType=IAC

McGovern, J., Ambler, S.W., Stevens, M.E., Linn, J., Sharan, V., and Jo, E.K. (2004) A Practical Guide to Enterprise Architecture. Prentice Hall. [242]

Mercuri, R. (2005) Security Watch: Challenges in Forensic Computing. Communications of the ACM, Volume 48 Issue 12. ACM Press. [17-21] Retrieved September 17, 2007 from http://delivery.acm.org.dml.regis.edu/10.1145/1110000/1101796/p17-mercuri.pdf?key1=1101796&key2=8394700911&coll=ACM&dl=ACM&CFID=30104998&CFTOKEN=11098819

Microsoft. (2008) Microsoft Solutions Finder: Partners Directory. Microsoft Corporation. Retrieved on January 16, 2008 from https://solutionfinder.microsoft.com/Partners/Directory/SeeAllTargetMarkets.aspx?sortby=relev_up&page=1&competency=120073aa9fff4a92bbd6548ff7965e95

Microsoft Technet. (2008) User State Migration Tool 3.0. Microsoft Corporation. Retrieved on February 21, 2008 from http://technet2.microsoft.com/WindowsVista/en/library/91f62fc4-621f-4537-b311-1307df0105611033.mspx?mfr=true

Microsoft Training and Certification. (1999) Implementing Microsoft Windows 2000 Professional and Server:Workbook Course Number 2152B. Microsoft Corporation. [Module12 5-6]

Preimesberger, C. (2007) Businesses Generally Ignoring E-Discovery Rules.

Ziff Davis CIO Insight. [1-2] Retrieved on January 2, 2008 from http://www.lexisnexis.com.dml.regis.edu/us/lnacademic/results/docview/docview.do?risb=21_T2773060824&format=GNBFI&sort=RELEVANCE&startDocNo=26&resultsUrlKey=29_T2773060827&cisb=22_T2773060826&treeMax=true&treeWidth=0&csi=262909&docNo=47

Probst, E. L., and Wright, K.A. (2006) Using their e-words against them. New Jersey Law Journal. LegalTrac. Gale. BCR Regis University. [1-5] Retrieved on January 2, 2008 from http://find.galegroup.com.dml.regis.edu/itx/retrieve.do?contentSet=IAC-Documents&resultListType=RESULT_LIST&qrySerId=Locale%28en%2C%2C%29%3AFQE%3D%28ke%2CNone%2C11%29E-Discovery%24&sgHitCountType=None&inPS=true&sort=DateDescend&searchType=AdvancedSearchForm&tabID=T002&prodId=LT&searchId=R1&currentPosition=51&userGroupName=regis&docId=A141430782&docType=IAC

Schwalbe, K. (2005) Information Technology Project Management. (4th ed.). Boston, MA: Thompson Course Technology. [175-179]

Shelton, G. D. (2006) Don't let the terabyte you: new e-discovery amendments to the federal rules of civil procedure. Defense Counsel Journal. LegalTrac. Gale. BCR Regis University. [324, 326, 237, 331] Retrieved on January 2, 2008 from

http://find.galegroup.com.dml.regis.edu/itx/retrieve.do?contentSet=IAC-Documents&resultListType=RESULT_LIST&qrySerId=Locale%28en%2C%2C%29%3AFQE%3D%28ke%2CNone%2C11%29E-Discovery%24&sgHitCountType=None&inPS=true&sort=DateDescend&searchType=AdvancedSearchForm&tabID=T002&prodId=LT&searchId=R1&currentPosition=31&userGroupName=regis&docId=A153361918&docType=IAC

Sherman, J. D., and Steidl, L.E. (2007) Discovery savings. New Jersey Law Journal. LegalTrac. Gale. BCR Regis University. [1-3] Retrieved on January 2, 2008 from http://find.galegroup.com.dml.regis.edu/itx/retrieve.do?contentSet=IAC-Documents&resultListType=RESULT_LIST&qrySerId=Locale%28en%2C%2C%29%3AFQE%3D%28ke%2CNone%2C11%29E-Discovery%24&sgHitCountType=None&inPS=true&sort=DateDescend&searchType=AdvancedSearchForm&tabID=T002&prodId=LT&searchId=R1&currentPosition=12&userGroupName=regis&docId=A163283447&docType=IAC

Steel, C. (2006) WINDOWS FORENSICS The Field Guide for Conducting Corporate Computer Investigations. Wiley Publishing, Inc. [25-26, 52, 194, 339]

Symantec Corporation. (2004) Norton Ghost User's Guide. Symantec Corporation. [38-42].

Wang, W. (2006) Steal This Computer Book 4.0. No Starch Press, Inc. [313-314, 318]

Weaver, R. (2007) Guide To Network Defense And Countermeasures 2nd Edition. Thomson Course Technology. [65, 84-86, 96]

Wires, J., Feeley, M. J. (2007) Secure File System Versioning at the Block Level. ACM SIGOPS Operating Systems Review, Proceedings of the 2007 conference on EuroSys EuroSys '07, Volume 41, Issue 3. [203, 214] Retrieved September 17, 2007 from http://delivery.acm.org.dml.regis.edu/10.1145/1280000/1273018/p203-wires.pdf?key1=1273018&key2=7785700911&coll=ACM&dl=ACM&CFID=30104998&CFTOKEN=11098819

Yeager, R. (2006) Student Papers: Criminal Computer Forensics Management. Proceedings of the 3rd annual conference on Information security curriculum development InfoSecCD '06. ACM Press. [168-170] Retrieved September 17, 2007 from http://delivery.acm.org.dml.regis.edu/10.1145/1240000/1231085/p168-yeager.pdf?key1=1231085&key2=0284700911&coll=ACM&dl=ACM&CFID=30104998&CFTOKEN=11098819

Zhu, Q., Hsu, W. W. (2005) Research Papers: Correctness and Trust: Fossilized

Index: The linchpin of trustworthy non-alterable electronic records. Proceedings of the 2005 ACM SIGMOD international conference on Management of data SIGMOD '05. ACM Press. [395-406] Retrieved September 17, 2007 from http://delivery.acm.org.dml.regis.edu/10.1145/1070000/1066203/p395-zhu.pdf?key1=1066203&key2=9964700911&coll=ACM&dl=ACM&CFID=30104998&CFTOKEN=11098819

Annotated Bibliography:

Adelstein, Frank. (2006) Next-generation Cyber Forensics: Live Forensics: Diagnosing Your System Without Killing It First. Communications of the ACM, Volume 49 Issue 2. [65] Retrieved September 17, 2007 from http://delivery.acm.org.dml.regis.edu/10.1145/1120000/1113070/p63-adelstein.pdf?key1=1113070&key2=5215700911&coll=ACM&dl=ACM&CFID=30104998&CFTOKEN=11098819

This document provides a perspective on the changing storage environment over time with particular emphasis on information availability from live systems that are running services, network connections and accessed by users. Emphasis is placed on the principles of order of volatility with regard to gathering data for forensic analysis and the timeliness of gathering memory dumps early on in any type of investigation and analysis.

Baron, Jason R., Thompson, Paul. (2007). Legal Information Retrieval: The search problem posed by large heterogeneous data sets in litigation: possible future approached to research. Proceedings of the 11th international conference on Artificial intelligence and law ICAIL '07. ACM Press. [141] Retrieved September 23, 2007 from http://delivery.acm.org.dml.regis.edu/10.1145/1280000/1276344/p141-baron.pdf?key1=1276344&key2=9644700911&coll=ACM&dl=ACM&CFID=30104998&CFTOKEN=11098819

This document discusses the problem posed by the increases in volume associated with discovery of information during civil litigation. The authors present the problem associated with

searches for data and the nature of the search task; how these searches are conducted; evaluation of data challenges; and the issue with missed searches for specific data types and documents. The information provides excellent background relating to the problem however; the proposal of the benchmarking of data retrieval through artificial intelligence is focused on the ability to accurately discover data by litigators rather than the importance of assuring compliance with simply making the data available.

Becerra-Fernandez, Irma., Gonzalez, Avelino., Sabherwal, Rajiv. (2004) Knowledge Management: Challenges, Solutions, and Technologies. Pearson Prentice Hall. Pearson Education Inc. [213]

This text addresses the challenges, solutions and technologies associated with knowledge management. While the primary topic of the text is in defining how to define what knowledge is, how to gather knowledge, and how to implement and use knowledge based systems; the key basic elements of the text deal with technologies and practices for capture and retrieval of data. As the authors present the case that knowledge is simply data put into context, much of the material surrounding the capture and management of data for knowledge systems is also applicable to capturing data for collections purposes towards compliance.

Burke, Christy. (2007) Examining e-discovery chain of custody. New Jersey Law Journal. LegalTrac. Gale. BCR Regis University. [1-3] Retrieved on January 2, 2008 from http://find.galegroup.com.dml.regis.edu/itx/retrieve.do?contentSet=IAC-Documents&resultListType=RESULT_LIST&qrySerId=Locale%28en%2C%2C%29%3

AFQE%3D%28ke%2CNone%2C11%29E-Discovery%24&sgHitCountType=None&inPS=true&sort=DateDescend&searchType=AdvancedSearchForm&tabID=T002&prodId=LT&searchId=R1&currentPosition=3&userGroupName=regis&docId=A170240519&docType=IAC

This text provides reference to chain of custody issues and recommendations for best practices in handling the chain of custody for electronic computer data evidence. The paper is presented from the perspective of the importance of the role of chain of custody procedures in handling evidence where failure to handle the evidence properly can make or break a legal case. The paper also expands on not only the handling of the data itself, but also in how the machinery that contains the data storage device should be handled and the ramifications for failure to properly handle the equipment under chain of custody procedures.

Butler, Chris, CISSP., Rogers, Russ, CISSP., Ferratt, Mason, JNCIS-FWV., Miles, Greg, CISSP., Fuller, Ed., Hurley, C., IAM/IEM., et al. (2007) IT Security Interviews Exposed. Wiley Publishing Inc. [49, 54-55, 61]

The majority of the authors are Certified Information Systems Security Professionals (CISSP) and all work within some area of relevance to the information security industry. The interviews within this book address a number of topics ranging from guidance towards regulations and legislation compliance to ethical considerations in information security investigations. The authors cover topics relating to data classification and labeling, backup and restoration of electronic data, and the impact of regulatory compliance on an organization.

Carvey, Harlan. (2007) Windows Forensic Analysis Incident Response and Cybercrime Investigation Secrets. Syngress Publishing, Inc. [128, 230, 232, 238, 263]

This book addresses the topics of analysis from data stored within volatile memory, to registry and file analysis. The book provides an in depth look at metadata and analysis of electronic file metadata for Microsoft Word documents and Portable Document Format (PDF) files. The author is a Certified Information Systems Security Professional and serves as a forensic analysis and incident response consultant based out of the metropolitan DC area. Mr. Carvey obtained his bachelor's degree in electrical engineering from Virginia Military Institute and his Master's degree in electrical engineering from the Naval Postgraduate School.

Casey, Eoghan. (2006) Next-generation Cyber Forensics: Investigating Sophisticated Security Breaches. Communications of the ACM, Volume 49 Issue 2. [50-51] Retrieved September 17, 2007 from http://delivery.acm.org.dml.regis.edu/10.1145/1120000/1113068/p48-casey.pdf?key1=1113068&key2=7025700911&coll=ACM&dl=ACM&CFID=30104998&CFTOKEN=11098819

This document details the importance of evidence preservation through logging and backup systems focused on the gathering of complete and accurate copies. Other emphasis includes the need for proper documentation for verification of the evidence and the collection process. The paper's focus is application of this principle in gathering evidence associated with intrusions and how to follow the cybertrail left by the perpetrator however; the principle provides support for the application of these processes towards proactive collection of data beyond the criminal investigation.

CommVault. (2007) CommVault Solutions – Legal Discovery. CommVault. Retrieved June 18, 2007 from

http://www.commvault.com/solutions/legaldisc/index.asp

This document provides a general data flow diagram which snapshots the problem with emphasis on the key areas of the rules amendments directly related to electronic legal discovery. From a high level view, this provides a very basic framework but only a very basic framework which may be expanded upon in greater detail for greater applicability in the enterprise.

Cornell Law School. (2007) Federal Rules of Civil Procedure Contents and Context. LII / Legal Information Institute. [Rule 26, Rule 34], Retrieved June 20, 2007 from

http://www.law.cornell.edu/rules/frcp/

This document provides the specific text for rules 26 and 34 of the Federal Rules of Civil Procedure (FRCP) including their amendments for electronic discovery. The specific text details exactly how the discovery process work within the federal courts however; like most areas of law, the language is subject to interpretation based on the text and all precedents established in case rulings.

Eriksson, Hans-Erik., Penker, Magnus ., Lyons, Brian., Fado, David. (2003) UML 2 Toolkit. New York: John Wiley & Sons. [1, 29-30, 58-63, 145-149]

This book provides reference and a foundation for the application of Unified Modeling Language (UML) in diagramming dataflow diagrams, use case scenarios, entity relationship diagrams, and documentation through modeling virtually any type of enterprise architecture model. The

application of UML is becoming a widely accepted practice for conveying information systems requirements, design, and implementation in a language that may be understood by both business stakeholders and engineers alike.

Francia, Guillermo, A., Clinton, Keion. (2005) Computer Forensics Laboratory and Tools. Journal of Computing Sciences in Colleges, Volume 20 Issue 6. [143-147] Retrieved September 17, 2007 from http://delivery.acm.org.dml.regis.edu/10.1145/1070000/1060428/p143-francia.pdf?key1=1060428&key2=9005700911&coll=ACM&dl=ACM&CFID=30104998&CFTOKEN=11098819

This document discusses the skills and training necessary for computer security professionals to perform the tasks of identification, preservation, and analysis of information stored and transmitted by a computer on or off of a network. The paper also presents recommendations for the establishment of a computer forensics laboratory. While the application is centered upon forensics from a criminal investigation perspective, the reference provides interesting topics for applicability beyond the criminal investigation process including the forensic analysis process and methodology and application of these methods to handling electronic data.

Friedman, Lawrence M. (2007) A History of American Law Third Edition. Touchstone A Division of Simon & Schuster, Inc. [516-537]

This book provides a history of the Unites States legal system. Part IV Chapter 2 deals specifically with the history of the legal system in the twentieth century and the increase in liability suits. This provides excellent support for the problem of discovery which defined the

rules by which legal council finds evidence to support and affirm liability on the defense. There is not a major focus on electronic data however; the material presents the greater problem an organization may face with liability claims within the U.S. court system including background on the explosion of TORT Laws and liability suits in the twentieth century.

Gallagher, Mary Pat. (2007) No computer tampering proved in test case of e-discovery rules.(New Jersey). New Jersey Law Journal. LegalTrac. Gale. BCR Regis University. [1-2] Retrieved on January 2, 2008 from http://find.galegroup.com.dml.regis.edu/itx/retrieve.do?contentSet=IAC-Documents&resultListType=RESULT_LIST&qrySerId=Locale%28en%2C%2C%29%3AFQE%3D%28ke%2CNone%2C11%29E-Discovery%24&sgHitCountType=None&inPS=true&sort=DateDescend&searchType=AdvancedSearchForm&tabID=T002&prodId=LT&searchId=R1&currentPosition=21&userGroupName=regis&docId=A158947863&docType=IAC

This paper discusses the elements of the Federal Rules of Civil Procedure regarding safe harbor and good faith attempts to meet court demands where such attempts can minimize risk in failing to provide the data requested. The paper further expands on the issue of data retention policies, lack of such policies, and the ramifications of retaining unnecessary data for unspecified lengths of time where that data could eventually serve to cause harm to the business.

Gasser, Urs., Haeusermann, Daniel. (2007) E-Compliance: Towards a Roadmap for Effective Risk Management. The Berkman Center for Internet & Society at Harvard Law School. Research Publication No. 2007-3. [4, 9, 17, 19] Retrieved July 17, 2007 from

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=971848

This research publication provides an excellent overview of risk management by transitioning from the traditional business compliance framework to an electronic compliance framework addressing compliance risk areas, security, data privacy, consumer protection, intellectual property and copyright law, and content governance. Additional information is presented regarding global issues with international law, ethics, and the growing significance of what the authors define as "soft law" or non-legally binding norms such as standards, codes of conduct, rules, and best practice models.

Gottschalk, Larry., Liu, Jigang., Dathan, Brahma., Fitzgerald, Sue., Stein, Michael. (2005) Computer Forensics Programs in Higher Education: A Preliminary Study. ACM SIGCSE Bulletin, Proceedings of the 36th SIG CSE technical symposium on Computer science education SIG CSE '05, Volume 37 Issue 1. ACM Press. [147] Retrieved September 17, 2007 from

http://delivery.acm.org.dml.regis.edu/10.1145/1050000/1047403/p147-gottschalk.pdf?key1=1047403&key2=9454700911&coll=ACM&dl=ACM&CFID=30104998&CFTOKEN=11098819

This study provides an argument for computer forensics programs as a higher discipline worthy of treatment as an independent field where currently computer forensics is regarded as a subfield under other disciplines such as criminology or information systems security. The authors present statistics for existing computer forensics programs of study at the undergraduate and graduate levels which provides interesting reference to the skills sets necessary to perform proper forensic investigations. The argument for the field of computer forensics as a primary discipline in itself

may be arguable however; the areas of coursework provided do point the reader in some interesting topic areas worth investigation for their applicability.

Grance, T., Hash J., Stevens M. (June 2004) Security Considerations in the Information System Development Life Cycle. NIST. Technology Administration U.S. Department of Commerce. [5, 31-33] Retrieved March 23, 2005 from http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf

The authors work for the National Institute of Standards and Technology (NIST) and this document provides a framework for implementing security considerations early in the System Development Life Cycle (SDLC) process. This document was created in furtherance of NIST's statutory responsibility under the Federal Information Security Management Act (FISMA) for developing standards and guidelines for provision of adequate standards and requirements for all agency operations and assets. Topics covered include general information security, control of data and information, legal issues, personnel security, and security documentation.

Hartwig, Robert PhD., Hudgins IV Esq., John M. "Skip"., McAuliffe, Timothy., Woollams, Richard. (2007) U.S. Tort System 2007: How rough is the ride ahead? American Tort Reform Association. [4] Retrieved July 17, 2007 from http://www.aigamericanhome.com/americanhome/public/ahafiledownload/0,1841,1164,00.pdf

This paper presents information regarding the cost implications associated with civil cases in the U.S. Tort system. This provides excellent reference of case information to the potential risks in terms of costs to an organization from judgments rendered against the organization by jurors and

judges. The paper also discusses the controversy of how far this practice should be pushed and if an organization can actually manage these changes. The paper presents excellent information for reference however; raises questions rather than providing solutions but can serve as an aid in establishing a business case for addressing the risk.

Hill, Steven. (2006) Policy Workbook: E-Discovery. Network Computing. CMP Media LLC. [37-39] Retrieved on January 2, 2008 from http://www.lexisnexis.com.dml.regis.edu/us/lnacademic/results/docview/docview.do?risb=21_T2773060824&format=GNBFI&sort=RELEVANCE&startDocNo=1&resultsUrlKey=29_T2773060827&cisb=22_T2773060826&treeMax=true&treeWidth=0&csi=155287&docNo=14

This paper discusses the implementation of an e-discovery program within an organization including key topics of consideration such as establishing procedures, policies, identification of stakeholders, qualifications of those stakeholders, and the process of initiating a legal hold of data within the enterprise once data has been subpoenaed by the court system. The also paper provides a reference to the activities in relation to the specific provisions and sections of the Federal Rules of Civil Procedure that apply to electronic discovery.

Jones, Keith J., Bejtilich, Richard., Rose, Curtis W. (2006) Real Digital Forensics Computer Security and Incident Response. [163-169] Pearson Education Inc.

Keith Jones is a director at Red Cliff Consulting LLC and has over eight years experience in computer incident and response. Mr. Jones holds two Bachelor of Science degrees in electrical engineering and computer engineering and also holds a Master's degree in electrical engineering

from Michigan State University. He is also a member of the Institute of Electrical and Electronics Engineers (IEEE). Richard Bejtich is the founder of TaoSecurity, a company that helps remediate intrusions through network monitoring solutions. Curtis Rose is an executive vice president of Red Cliff Consulting LLC, a company that provides information security, incident response, forensics analysis, and education services. This book addresses real world application of techniques and processes for recovery of deleted files, activity reconstruction, registry analysis and reconstruction, analysis of forensic tools, and is one of the few texts that actually address the topic of E-Discovery.

Lagerweij, B. (2000-2008) Bart's Preinstalled Environment (BartPE) bootable live windows CD/DVD. NU2 Website. Retrieved on February 24, 2008 from http://www.nu2.nu/pebuilder/

This website provides reference information regarding Bart's Preinstalled Environment which allows for the creation of stand alone bootable Windows installations for the purposes of creating bootable CD-ROM, DVD-ROM, or Flash media drives. The PE Builder allows for creation of a Win32 environment with networking support, graphical user interface, and FAT/NTFS/CDFS file system support. The limitations of a DOS bootable floppy disk are a thing of the past with the PE Builder which will allow for creation of a Windows bootable that may be customized to include virtually any software tool that is capable of running on a standard Windows environment.

Lang, Joseph P., and Baffa, James. (2007) Electronic Discovery: An Overview And Practical Pointers. Bates & Carey LLP. Retrieved September 23, 2007 from

http://www.batescarey.com/newsandarticles/electronicdiscovery.asp

This document provides and overview of rulings and damages relating to electronic discovery. The paper is presented by a law firm which could denote bias however; the specific cases presented also provide their specific case numbers for reference to the actual court cases.

Lexis Nexis® (2007) Federal Rules of Civil Procedure.

LexisNexis, a division of Reed Elsevier Inc. Retrieved April 30, 2006 from

http://www.lexisnexis.com/lawschool/learning/reference/pdf/2006/LA11909-0_FRCP.pdf

This reference is the entire text of the revised Federal Rules of Civil Procedure (FRCP) which provides the framework by which civil cases are handled within the federal court system. Many States align their processes with the FRCP for State civil courts. The entire text provides the rules attorneys are expected to follow during a civil suit. The specific references to electronic discovery under rules 26 and 34 are the most important references however; the complete rules provides a reference for rules which may provide information essential to the establishment of policies and procedures which may be used to place the rule argument under another rule context all together as a defense.

Marean, Browning. (2007) E-discovery looks like risky business. New Jersey Law Journal. LegalTrac. Gale. BCR Regis University. [1-2] Retrieved on 2 January 2, 2008 from

http://find.galegroup.com.dml.regis.edu/itx/retrieve.do?contentSet=IAC-Documents&resultListType=RESULT_LIST&qrySerId=Locale%28en%2C%2C%29%3AFQE%3D%28ke%2CNone%2C11%29E-

Discovery%24&sgHitCountType=None&inPS=true&sort=DateDescend&searchType=AdvancedSearchForm&tabID=T002&prodId=LT&searchId=R1&currentPosition=1&userGroupName=regis&docId=A170459778&docType=IAC

This paper discusses the challenges posed to both legal and IT professionals when it comes to e-discovery. Elements of the paper's topic include the issue of determining when litigation may be anticipated, sanctions imposed by the courts for failing to meet e-discovery requests, the risks to the process that exist early in the process, and key elements to consider to minimize such risks.

McGovern, J., Ambler, S.W., Stevens, M.E., Linn, J., Sharan, V., and Jo, E.K. (2004) A Practical Guide to Enterprise Architecture. Prentice Hall. [242]

This book provided an overview of several enterprise architecture models and methodologies including management of the information systems environment under these different types of architecture models. This book not only focuses on what the methodologies are but also how they should be documented.

Mercuri, Rebecca. (2005) Security Watch: Challenges in Forensic Computing. Communications of the ACM, Volume 48 Issue 12. ACM Press. [17-21] Retrieved September 17, 2007 from http://delivery.acm.org.dml.regis.edu/10.1145/1110000/1101796/p17-mercuri.pdf?key1=1101796&key2=8394700911&coll=ACM&dl=ACM&CFID=30104998&CFTOKEN=11098819

This paper presents the challenges associated with the ever changing technology which has forced computer forensics to move beyond an ad hoc process to a more recognized discipline.

The paper is focuses heavily on the rules of evidence in court cases with particular emphasis on handling data, making full mirror copies of data, and preservation of audit trails for how the data is handled.

Microsoft. (2008) Microsoft Solutions Finder: Partners Directory. Microsoft Corporation. Retrieved on January 16, 2008 from https://solutionfinder.microsoft.com/Partners/Directory/SeeAllTargetMarkets.aspx?sortby=relev_up&page=1&competency=120073aa9fff4a92bbd6548ff7965e95

This webpage provides a reference for determination of company size as interpreted by the Microsoft Partner's Directory. This will aid in determining company sizes in analyzing survey results.

"Enterprise Business – over 1000 employees."

"Mid-market Business- 50-1000 employees."

"Small Business – 1-49 employees."

Microsoft Technet. (2008) User State Migration Tool 3.0. Microsoft Corporation. Retrieved on February 21, 2008 from http://technet2.microsoft.com/WindowsVista/en/library/91f62fc4-621f-4537-b311-1307df0105611033.mspx?mfr=true

This webpage provides resource information for how Microsoft's User State Migration Tool 3.0 functions. The tools primary objective is for migrating individual user settings and documents from one system to another during large deployments of Microsoft Windows XP and Vista operating systems migrations and upgrades.

Microsoft Training and Certification. (1999) Implementing Microsoft Windows 2000 Professional and Server:Workbook Course Number 2152B. Microsoft Corporation. [Module12 5-6]

This course manual provides an overview of the NTFS operating system protocol including permissions management, inheritance, and disk configurations. This book provides a differentiation between basic and dynamic disk volumes and how they are configured including references to RAID-5.

Preimesberger, Chris. (2007) Businesses Generally Ignoring E-Discovery Rules. Ziff Davis CIO Insight. [1-2] Retrieved on January 2, 2008 from http://www.lexisnexis.com.dml.regis.edu/us/lnacademic/results/docview/docview.do?risb=21_T2773060824&format=GNBFI&sort=RELEVANCE&startDocNo=26&resultsUrlKey=29_T2773060827&cisb=22_T2773060826&treeMax=true&treeWidth=0&csi=262909&docNo=47

This paper discusses and presents statistics regarding the Federal Rules of Civil Procedure requirements for establishment of policies for data retention and the ability to clearly cite and demonstrate those policies to the court. The paper also discusses the lack of awareness to the e-discovery issue and some of the reasons for this lack of awareness.

Probst, Eric L., and Kerri A. Wright. (2006) Using their e-words against them. New Jersey Law Journal. LegalTrac. Gale. BCR Regis University. [1-5] Retrieved on January 2, 2008 from

http://find.galegroup.com.dml.regis.edu/itx/retrieve.do?contentSet=IAC-Documents&resultListType=RESULT_LIST&qrySerId=Locale%28en%2C%2C%29%3AFQE%3D%28ke%2CNone%2C11%29E-Discovery%24&sgHitCountType=None&inPS=true&sort=DateDescend&searchType=AdvancedSearchForm&tabID=T002&prodId=LT&searchId=R1&currentPosition=51&userGroupName=regis&docId=A141430782&docType=IAC

This paper discusses the use of e-discovery by businesses against plaintiffs who would use the Federal Rules of Civil Procedure rules changes regarding electronic discovery such that the same rules may be applied to individual plaintiffs as a tactic to encourage settlement, discredit of the plaintiff, or dropping of the case all together.

Schwalbe, K. (2005) Information Technology Project Management. (4th ed.). Boston, MA: Thompson Course Technology. [175-179]

Kathy Schwalbe is an Associate Professor in the Department of Business Administration at Augsberg College in Minneapolis Minnesota. The text is based upon the Project Management Body of Knowledge (PMBOK) Guide 2004 from the Project Management Institute (PMI). This book details an introduction into information technology project management and then describes each of the project management knowledge areas for project integration, scope, time, cost, quality, human resource, communications, risk management, and procurement management.

Shelton, Gregory D. (2006) Don't let the terabyte you: new e-discovery amendments to the federal rules of civil procedure. Defense Counsel Journal. LegalTrac. Gale. BCR Regis University. [324, 326, 237, 331] Retrieved on January 2, 2008 from

http://find.galegroup.com.dml.regis.edu/itx/retrieve.do?contentSet=IAC-Documents&resultListType=RESULT_LIST&qrySerId=Locale%28en%2C%2C%29%3AFQE%3D%28ke%2CNone%2C11%29E-Discovery%24&sgHitCountType=None&inPS=true&sort=DateDescend&searchType=AdvancedSearchForm&tabID=T002&prodId=LT&searchId=R1&currentPosition=31&userGroupName=regis&docId=A153361918&docType=IAC

This document presents a perspective on the volume of electronic data and storage for such data. The paper also discusses the safe harbor provisions within the Rules such that routine operation is better understood in regard to data retention, overwritten and deleted data. The author also provides a definition of the terabyte unit of measurement for electronic file storage and a comparison to paper document counterparts. Other topics covered include the definition for "good faith operations" under the Federal Rules of Civil Procedure.

Sherman, James D., and Steidl, Lori, E. (2007) Discovery savings. New Jersey Law Journal. LegalTrac. Gale. BCR Regis University. [1-3] Retrieved on January 2, 2008 from http://find.galegroup.com.dml.regis.edu/itx/retrieve.do?contentSet=IAC-Documents&resultListType=RESULT_LIST&qrySerId=Locale%28en%2C%2C%29%3AFQE%3D%28ke%2CNone%2C11%29E-Discovery%24&sgHitCountType=None&inPS=true&sort=DateDescend&searchType=AdvancedSearchForm&tabID=T002&prodId=LT&searchId=R1&currentPosition=12&userGroupName=regis&docId=A163283447&docType=IAC

This paper discusses then issues and benefits of reviewing data in its native formats versus the expense of document conversions including audit trails, metadata review, and cost implications

associated with extensive document conversions as an undue hardship on a business. The paper also discusses rule 26(f) of the Federal Rules of Civil Procedure where the format that documents are to be delivered in is agreed upon early in the process as part of the procedure.

Steel, Chad. (2006) WINDOWS FORENSICS The Field Guide for Conducting Corporate Computer Investigations. Wiley Publishing, Inc. [25-26, 52, 194, 339]

Chad Steel developed and taught the Computer Forensics graduate courser in Penn State's engineering program and has experience investigating more than 300 computer security incidents. Mr. Steel holds Bachelor's and Master's degrees in computer engineering. This book presents information related to corporate computer forensic analysis including the concept of "best evidence" and the importance of chain of custody in the handling of the electronic data. Key topics include forensic duplication of hard drives, media for duplication, covert analysis, overt analysis, and Internet usage analysis. The book also addresses analysis for email investigations and addresses such technical data as FAT32 boot sector layout, NTFS boot sector layout, partition types, and master boot record layout. This is an excellent reference book that deals specifically with the Windows operating system.

Symantec Corporation. (2004) Norton Ghost User's Guide. Symantec Corporation. [38-42].

This book provides specific detail for the use of the Norton Ghost version 9.0 image capture software. The guide details how to use the application for snapshot of a computer hard drive, restoring files and folders from an image, restoring backup images, use of the tool over a network environment, and exploring an image file.

Wang, Wallace. (2006) Steal This Computer Book 4.0. No Starch Press, Inc. [313-314, 318]

This book addresses the topic of "hacking and hackers". Much of the information is focused on developing the reader's knowledge of the hacker community with focus on viruses, Trojans, spyware, adware, intrusion detection, password cracking, and other vulnerabilities however; certain topics that pose excellent reference for the topic of discovery include file sharing networks, retrieval of deleted data, forensics tools, and censoring information. This reference provides explanation for how data is deleted from a Windows based computer and more importantly, what is left behind.

Weaver, Randy. (2007) Guide To Network Defense And Countermeasures 2nd Edition. Thomson Course Technology. [65, 84-86, 96]

This book is intended for students and professionals who need or desire, a hands-on introductory experience to installing network intrusion detection systems and firewalls. The book's primary topic is focused upon network defense and countermeasures however; certain topics relating to management principles, incident response, virtual private networking, risk analysis, and policy design may be expanded upon into the areas of the desktop architecture for discovery and collections.

Wires, Jake., Feeley, Michael, J. (2007) Secure File System Versioning at the Block Level. ACM SIGOPS Operating Systems Review, Proceedings of the 2007 conference on EuroSys EuroSys '07, Volume 41, Issue 3. [203, 214] Retrieved September 17, 2007 from

http://delivery.acm.org.dml.regis.edu/10.1145/1280000/1273018/p203-wires.pdf?key1=1273018&key2=7785700911&coll=ACM&dl=ACM&CFID=30104998&CFTOKEN=11098819

This paper presents the vulnerabilities associated with the risk of data being overwritten or deleted either accidentally or by malicious intent. While the paper is presented from a perspective of the implementation of a prototype evaluation system for file versioning at the block level; the topics relating to versioning, retrieval, consistency, deletion, and verification all have relevance to the collection of electronic data. The paper is heavily biased to support the conclusions for the prototype system VDisk as a solution to block level data retrieval. But the topics within the paper when taken in context, are a valuable resource beyond the author's conclusions.

Yeager, Ray. (2006) Student Papers: Criminal Computer Forensics Management. Proceedings of the 3rd annual conference on Information security curriculum development InfoSecCD '06. ACM Press. [168-170] Retrieved September 17, 2007 from http://delivery.acm.org.dml.regis.edu/10.1145/1240000/1231085/p168-yeager.pdf?key1=1231085&key2=0284700911&coll=ACM&dl=ACM&CFID=30104998&CFTOKEN=11098819

This research paper addresses the methodologies and approaches to managing criminal computer forensic investigations. A definition of what forensics as a science is presented with policies, procedures, rules, and standards. The paper is focused on defining how to manage this process. The author focuses specifically on the use of this methodology within criminal investigations for

law enforcement however; these same principles may serve as the basis for any corporate practice as well as data collections for civil cases.

Zhu, Qingbo., Hsu, Windsor, W. (2005) Research Papers: Correctness and Trust: Fossilized Index: The linchpin of trustworthy non-alterable electronic records. Proceedings of the 2005 ACM SIGMOD international conference on Management of data SIGMOD '05. ACM Press. [395-406] Retrieved September 17, 2007 from http://delivery.acm.org.dml.regis.edu/10.1145/1070000/1066203/p395-zhu.pdf?key1=1066203&key2=9964700911&coll=ACM&dl=ACM&CFID=30104998&CFTOKEN=11098819

This paper presents that electronic record storage is vulnerable to ease of destruction and manipulation and further contends that the storage of records in WORM storage is far more inadequate a solution than regulators believe it to be. The authors present that the trustworthiness of data is an end to end process and the digital backup alone does not provide enough trustworthiness to refute challenge. The paper primarily attacks the basis of WORM storage as an adequate storage medium for compliance with regulatory requirements however; their case in a broader perspective supports the end to end process management beyond WORM storage devices.

Glossary of Terms

APEX	Application Express
CCTV	Closed Circuit Television
CD	Compact Disk
CFR's	Code of Federal Regulations
DVD	Digital Versatile Disk
EDD	Electronic Data Discovery
E-Discovery	Electronic Discovery
FRCP	Federal Rules of Civil Procedure
GMT	Greenwich Mean Time
IDE	Integrated Drive Electronics
Infosec	Information Security
IS	Information Systems
ISP	Internet Service Provider
IT	Information Technology
MAC	Modified Accessed Created
NetApp	Network Appliance
NIST	National Institute of Standards and Technology
NTFS	NT File System
OLE	Object Linking and Embedding
OS	Operating System
PDA	Personal Digital Assistant
PDF	Portable Document Format
PE	Preinstallation Environment
RAID	Redundant Array of Inexpensive Disks
ROM	Read Only Memory
SCSI	Small Computer System Interface
SDLC	System Development Life Cycle
SMS	System Management Server
UML	Unified Modeling Language
USB	Universal Serial Bus
UTC	Coordinated Universal Time