

WEBSTER UNIVERSITY
School of Business and Technology

Doctoral Project Committee

Albert J. Marcella, Jr., Ph.D. – Chairperson
D. Christopher Risker, Ph.D.
Barrett Baebler, D.Mgt.
Patrick M. Flachs, J.D.

Electronic Discovery:
Awareness of
The Recently Enacted Federal Rules of Civil Procedure (FRCP)
And Impact on Enterprise Risk

by

Shirley Jutras Fitzgerald

A doctoral project presented to
the School of Business & Technology
At Webster University
in partial fulfillment of the requirements for the degree
Doctor of Management

September, 2008
St. Louis, Missouri

UMI Number: 3334121

INFORMATION TO USERS

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleed-through, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

UMI[®]

UMI Microform 3334121

Copyright 2009 by ProQuest LLC.

All rights reserved. This microform edition is protected against unauthorized copying under Title 17, United States Code.

ProQuest LLC
789 E. Eisenhower Parkway
PO Box 1346
Ann Arbor, MI 48106-1346

© copyright by Shirley Jutras Fitzgerald
ALL RIGHTS RESERVED
(2008)

WEBSTER UNIVERSITY
DOCTOR OF MANAGEMENT

Doctoral Project Approval

To: John Patrick Orr, Ph.D.
Director
Doctor of Management Program

From: Doctoral Project Committee

Chair: Albert Marcella, Ph.D.

Member: Patrick M. Flachs, J.D.

Member: D. Christopher Risker, Ph.D.

Member: Barrett Baebler, D.Mgt.

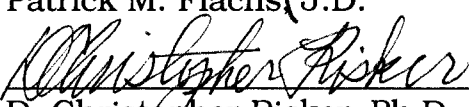
We, the Doctoral Project Committee, do certify that the Doctor of Management candidate:

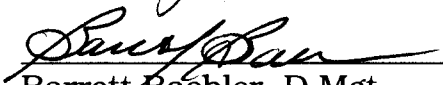
SHIRLEY FITZGERALD

has satisfactorily completed all requirements for the degree of Doctor of Management in the Doctoral Program at Webster University, and do, therefore recommend that this candidate be awarded the degree of Doctor of Management.

Chair:  Date: 9-29-08
Albert Marcella, Ph.D.

Member:  Date: 09-29-08
Patrick M. Flachs, J.D.

Member:  Date: 09-29-08
D. Christopher Risker, Ph.D.

Member:  Date: 9-29-08
Barrett Baebler, D.Mgt.

CONCURRENCE:

I do concur with the recommendations of the Doctoral Project Committee as stated above.

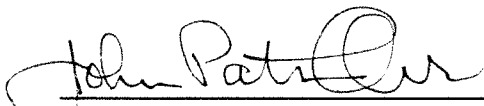

John Patrick Orr, Ph.D.
Director
Doctor of Management Program

TABLE OF CONTENTS

Abstract of Research Proposal	1
Chapter I – Introduction	2
The Problem	5
Preview of Existing Theory	7
The Purpose	8
Chapter II – Literature Review	9
The Need for Rules	10
Federal Rules of Civil Procedure – Proposed Amendments	11
Summary of Amendments	12
<i>General Provisions</i>	13
<i>Privileged Information and Work Products</i>	15
<i>Forms of Production</i>	16
<i>Preservation</i>	16
<i>Safe Harbor</i>	17
<i>Cost Shifting</i>	17
<i>Landmark Cases</i>	19
<i>Implications for Business</i>	22
Chapter III – Methodology	26
Research Objectives	26
Research Questions	27
Qualitative Research	27

Justification for the Research	29
The Research Plan	29
Potential Validity Concerns	33
Human Subjects Statement	34
Chapter IV – Findings	36
Data Collection	37
Summary of Interviews	40
Cyber-Forensics Survey	49
Statistical Analysis of Survey Results	63
Summary of Statistical Analysis	69
Summary of Findings	70
Chapter V – Conclusions	73
Research Goals	73
Interview Findings	73
Survey Results	76
Areas for Future Study	77
Recommendations	79
<i>Recommendations for Business</i>	81
<i>Recommendations for Counsel</i>	88
Summary and Conclusions	90
List of Appendixes	92
References	117

ABSTRACT OF THE RESEARCH PROPOSAL

**Electronic Discovery:
Awareness of
The Recently Enacted Federal Rules of Civil Procedure (FRCP)
and Impact on Enterprise Risk**

by

Shirley Jutras Fitzgerald

Student, Doctor of Management

Webster University in St. Louis (2008)

Chairperson: Albert J. Marcella, Jr., Ph.D.

Amendments to the Federal Rules of Civil Procedure (FRCP), as they relate to electronic data, were enacted into law on December 1, 2006. The amendments provided specific and detailed rulings regarding what constitutes electronic data as it pertains to the discovery process in litigation. The purpose of this study is to assess the level of awareness of the new amendments and their potential impact on enterprise risk. The research will consist of both qualitative and quantitative elements, including interviews and a survey questionnaire. Based on the results of a pilot study conducted over the course of several months in 2006-2007, this research is aimed at formalizing a theory regarding the level of awareness that currently exists at various levels of the enterprise.

Chapter I

INTRODUCTION

We woke up one day, and the Information Age was suddenly upon us – or so it seems, sometimes. But the fact of the matter is that it did not just happen overnight. Information, and the means by which we create and share it, have simply been evolving; and the pace of that evolution has been picking up momentum, particularly in the last few decades. We have gone from the quill, to the pen, to the computer; from Pony Express, to Air Mail, to e-mail. We have come to voice mail (VM), to instant messaging (IM), to BlackBerrys, to blogs and wikis. We have come to more information, more quickly, in more formats. What does all this mean? For many, it means a better quality of life; it means we have more resources at our disposal to help us live better and more productive lives. It means our businesses and our economies are growing at an unprecedented rate. It also means there is nowhere left to hide.

We have grown so accustomed to the sheer volume of information and communication that comes at us every day that we do not even think about it much. It just *is*. We leave voice mail messages, send e-mails, and text message one another without giving it a thought. We do it at home, we do it at work – and we do not think twice about commingling the two. In fact, many employees are firmly convinced that personal messages sent by means of company e-mail, company telephones, et cetera, are just that – *personal*. “[T]here is the sense that office PCs are exactly what the name implies: personal computers” (Sanders, 1999, p. 60). In a recent article titled, *Employees Don’t “Get” Electronic Storage*, Zeidner notes some interesting findings from a recent survey wherein, “more than

half of the respondents” did not understand the concept that anything you do by means of company resources (i.e., e-mail, IMs, voice mail, the Internet, et cetera) becomes a business record. And “[y]ounger workers (18-34) tended to be less aware than older ones. More than half of the younger group (55 percent) did not understand that sending an e-mail to a friend created a business record, compared with 39 percent of those over 55 ... The bottom line, says Marion Walker, senior counsel for the Ford & Harrison law firm in Birmingham, Ala., is clear: ‘Anyone who turns on an employer’s computer has no right to expect privacy’ ” (Zeidner, 2007, p. 36).

The other part employees “Don’t Get” is the fact that the company becomes liable for the content of those business records – just as they do for the content of all records that are created in the normal course of business. And while “[r]egulatory agencies encourage organizations to regularly disclose policies for e-mail management and instant messaging (IM) services,” enforcing compliance is another matter, and “can create enormous regulatory risk for the organization” (Rhinehart, 2006).

Today’s reality is that “93 percent of all business documents are created electronically” (Lange, 2003, p. 21). When coupled with the decreasing cost of storage, this allows “[t]oday’s ‘digital packrat’ [to] hoard astronomical quantities of electronic information ... According to a recent article in the Wall Street Journal, ‘We went through a belief that storage was cheap so we could save everything’ ... [and] although storage may be cheap or free ... it is not necessarily the wisest decision for an organization to make” (Myler, 2006, p. 52). Cautions Bandrowsky, who is Chief Operating Officer (COO) of Wescott Technology Services, LLC, “ ‘The

volume of data that must be managed or handled for litigation directly affects the cost of discovery' ” (Garretson, 2006, p. 83).

“In preparation for trial or other legal action, each party has the right to learn about, or discover, as much as possible about the opponent’s case. This pre-trial process is called discovery. A discovery request is an official request for access to any type of information that may be considered evidence ... Information is discoverable (i.e., subject to discovery) if it is relevant to the facts that lead to the lawsuit or litigation” (Volonino, 2003, p. 461). And in the eventuality of electronic discovery, or e-discovery, cost containment is the challenge.

“This is all based on an increasingly litigious environment” (Myler, 2006, p. 52). And if anything has kept pace with information’s growing momentum, it has been the growth rate of litigation. Which brings us to the topic at hand – E-Discovery. We are talking about electronically stored information, or ESI. “[W]ith regulations like SOX [Sarbanes-Oxley], corporate e-mail messages have achieved the same status as other commonly used business documents ... [which represents] a litigious gold mine of information for discovery in the event of a lawsuit” (Rhinehart, 2006). Furthermore, “Section 802 of SOX imposes fines of up to \$25 million and/or 20 years imprisonment against:

‘whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence’ any government investigation or official proceeding” (Volonino, 2003, p. 459).

As James Swann recently noted in his article, *E-mail Becomes Fair Game in Federal Court*, “[e]lectronically stored information, including e-mails, is now discoverable in federal court, due to amendments to the Federal Rules of Civil

Procedure that went into effect December 1, 2006” (2007, p. 58). These statutes “include more than just E-mail; they address anything that can be stored in any type of electronic manner” (Edwards, 2007, p. 25); they “widen the scope of electronic discovery to include home computers, text messages, PDAs and Internet Service Providers. All may be open to discovery during litigation now” (Lofton, 2007, p. 19). As the commercial goes, “you name it – it’s in there.”

Even though the amendments have already gone into effect, most legal counsel and business executives “have never heard of, much less prepared for, the impact of ESI. Indeed, ESI has not grabbed the headlines and garnered the attention that preceded the enactment of SOX, but it may well have a far more significant impact on how enterprises manage and control their exponentially growing stores of e-data” (Gibson, 2006, p. 5). And as with SOX, “[t]he Col. Klink Defense (‘I know nothing’) used by lawyers who claim they don’t possess or even know of certain documents will [now] hold less water” (Solnik, September/2006, p. 38).

“Welcome to ‘E-Discovery,’ a high-tech cross between the legal profession and the computer industry” (Solnik, September/2006, p. 38).

The Problem

“It’s been said that if it’s not documented, it didn’t happen” (Myler, 2006, p. 56). And document, we do. “According to the SIMS study [from the University of California at Berkeley], in 2002 alone, five exabytes of new data were created worldwide, which is equivalent to half a million new libraries the size of the Library of Congress print collection. Ninety-two percent of this new information was

electronic, stored primarily on hard disks” (Gibson, 2006, p. 5). Rick Wolf, former head of Cendant Corporation notes, “It’s analogous to the Industrial Revolution, when companies manufactured at a rapid pace irrespective of the effects of that activity on the environment, and we’re still cleaning it up today ... [Continues Wolf,] Most companies already own the technology that will solve their problems ... What they don’t have is a handle on their business processes and behavior” (Garretson, 2006, p. 89).

Sooner or later, every organization will have to face the need to produce ESI, and even though the new amendments to the Rules went into effect December 1, 2006, there are still a large number of organizations – along with their executives and counsel, alike – that do not have any idea what this means in terms of the potential impact on the businesses they run and represent. “Nothing has driven spending on IT security products and services over the past few years more than the need to comply with a flurry of new regulations ... including the Health Information Portability and Accountability Act (HIPPA), Sarbanes-Oxley (SOX), and Gramm-Leach-Bliley ... [and now,] the newly amended Federal Rules of Civil Procedure ... At the board level, executives want to know their level of risk related to compliance, so [chief information security officers], chief privacy officers, and chief risk officers have to be able to connect spending on IT security with meeting the demands of these various regulations” (Greenemeier, 2006, ¶ 3, 8). When you consider that “findings from the Fulbright & Jaworski survey indicate that large companies (more than \$1 billion) face an average of 556 lawsuits worldwide and spend an average of \$34 million on legal costs ... (Fulbright & Jaworski,

2006)” (Marcella, 2006, p. 7), this seems to be a very good time for them to start the work of finding out what they need to know and what they need to do about it.

Preview of Existing Theory

Based on the results of a pilot study conducted in late 2006 / early 2007, Marcella and Menendez postulate that, “as a discipline, the application of cyber forensics and the implementation of cyber forensic investigation techniques are in their infancy and *organizational awareness* to establishing and implementing policies and procedures dealing with the various elements of cyber forensics, almost nonexistent” (2008, p. 332). And while the authors note that the pilot sample size limits the generalizability and “broad applicability of the results revealed from this research, ... the basic findings clearly indicate that more work – and more research in this area – is warranted” (p. 341).

Many recent articles have referred to these times as the “Brave New World” of E-discovery (Garretson, 2006, p. 82; Marcus, 2006 [title], p. 635; and Solnik, December/2006, [title], p. 4B). But is the concept really new? Certainly, litigation is hardly new. The “Federal Rules of Civil Procedure became effective in 1938 ... [providing] for liberal discovery” (Cortese, 2005, p. 356). And while the Rules have been further expanded with amendments over the years, “Bill Savino, managing partner at Rivkin, Radler in Uniondale, called it a case of regulations catching up to change. ‘I think the rules of practice are now conforming to technology,’ Savino said. ‘E-Discovery is clearly upon us’ ” (Solnik, 2006/December, p. 4B). And, “[f]or better or worse, electronic data never really just goes away. For companies to meet regulatory requirements and protect themselves against litigation and other

losses, they need to be prepared to deal reactively and proactively with data demands” (Lewis & Gray, 2006, p. 44).

The Purpose

The purpose of this research proposal is to assess the level of awareness that exists among counsel and executive / senior level management regarding the newly enacted amendments to the Federal Rules of Civil Procedure (FRCP), and the potential impact those amendments will have on the enterprise in the event of litigation. In today’s increasingly litigious environment, it is no longer a question of *if* the enterprise will end up in discovery, it is a question of *when*. As we learn more about the level of awareness that exists at various levels of the enterprise, we will be better equipped to provide the tools needed to manage its risks.

A goal of this research is to develop a theory that will allow the researcher to better understand the relationships that exist between awareness of the Federal Rules of Civil Procedure (FRCP), the recently enacted amendments to the FRCP, their effect on organizational policy actions, and organizations’ preparedness to comply with the FRCP in the event of litigation involving electronic discovery.

Chapter II

LITERATURE REVIEW

The strategy employed in this literature review involved the process of researching, assembling, and documenting as much material as possible regarding the Federal Rules of Civil Procedure (FRCP), and the recently enacted amendments to same, involving searches on topics including, but not limited to:

- electronic discovery;
- digital forensics;
- computer forensics; and
- litigation cases involving electronic discovery.

While much has been written on this subject, to date no formal theories have been found regarding the level of awareness of the FRCP and the recently enacted amendments thereto. As can be seen in the following pages, most of the literature and theorizing have been more focused on the effects of the new legislation rather than on existing levels of awareness and their potential impact on those effects.

Many recent articles have referred to these times as the “Brave New World” of E-discovery (Garretson, 2006, p. 82; Marcus, 2006, [title] p. 635; and Solnik, December/2006, [title], p. 4B). But is the concept really new? Certainly, litigation is hardly new. The “Federal Rules of Civil Procedure became effective in 1938 ... [providing] for liberal discovery” (Cortese, 2005, p. 356). And while the Rules have been further expanded with amendments over the years, “Bill Savino, managing partner at Rivkin Radler in Uniondale, called it a case of regulations catching up to change. ‘I think the rules of practice are now conforming to technology,’ Savino said. ‘E-Discovery is clearly upon us’ ” (Solnik, 2006/December, p. 4B).

So why all the fuss? What started this snowball rolling down the hill?

“According to people involved in the move to get the rules adopted, the match that lit all this was struck in March 2000, when then-Vice President Al Gore reported that he could not immediately produce e-mails related to a probe by the Department of Justice into his fund-raising activities ... Afterward, a movement was started to shore up the court rules in this area” (Preimesberger, 2006, p. 11). That may well have been the match, but the fuel that keeps the fires burning comes from two sources – the rising costs of litigation, and the settlements and sanctions resulting from landmark cases such as *Rowe Entertainment Inc. v. William Morris Agency Inc.* and *Zubulake v. UBS Warburg LLC*. “The cost of e-discovery is skyrocketing. Estimated to be a \$2 billion industry in 2006, the cost of e-discovery is anticipated to grow by 35 percent a year” (Gibson, 2006, p. 6).

The Need for Rules

Along with changes in technology have come changes in the way we conduct the normal course of business. But “[t]he current discovery rules, last amended in 1970 to take into account changes in information technology, provide[d] inadequate guidance to litigants, judges, and lawyers in determining discovery rights and obligations in particular cases” (Cortese, 2005, p. 355). Case law was developing around local rules with inconsistencies that were “particularly confusing and debilitating to large public and private organizations, [with] the uncertainty, expense, delays, and burdens of such discovery also affect[ing] small organizations and individual litigants” (Cortese, 2005, p. 355). “Accordingly, the Conference of Chief Justices established a Working Group at its 2004 Annual Meeting to develop a reference document to assist state courts in considering

issues related to electronic discovery ... to offer guidance to those faced with addressing the practical problems that the digital age has created, and should be considered along with the other resources ... including the newly revised provisions on discovery in the Federal Rules of Civil Procedure and the most recent edition of the American Bar Association Standards Relating to Discovery” (Conference, 2006, p. vii).

The uncertainty surrounding the issues has also led to a certain amount of abuse. “In the past, lawyers have made broad and expansive discovery requests ... knowing how much it would cost the defendant to produce such information, review it for relevancy, copy it, and provide it. Settlement demands have actually been based on the estimated cost to comply with discovery rather than on the merits of the case” (E-Discovery Amendments to FRCP Approved, 2006, p. 15). Abuse aside, the sheer volume and lack of management of electronic data had in-house attorneys “reporting that 10 percent of cases against their companies [were] settled just to avoid the cost of e-discovery” (Gibson, 2006, p. 6). As Cyber Controls, LLC further notes, “Lawyers are fearful to launch an e-discovery request because they anticipate a boomerang request to be launched right back at their own client” (2008). The need for national rules and standards was rapidly becoming apparent.

Federal Rules of Civil Procedure – Proposed Amendments

The Civil Rules Advisory Committee “began intensive work on this subject in 2000 ... Study of the issues included several conferences that brought together lawyers, academics, judges, litigants, and experts in information technology with a variety of experiences and viewpoints” (Cortese, 2005, p. 355). Arguably the most

noteworthy, The Sedona Conference Working Group came together in October, 2002. The group consisted of attorneys and others experienced in matters of electronic discovery, with “the premise that electronic document production standards arising out of [their] practical experiences would bring needed predictability to litigants and guidance to courts” (The Sedona Conference, July/2005, p. iii). They recognized that electronic discovery should be “a tool to help resolve [disputes] and should not be viewed as a strategic weapon to coerce unjust, delayed, or expensive results” (p. iii). The fruits of their labor were “intended to complement the Federal Rules of Civil Procedure,” and The Sedona Principles were first published in January, 2004 (p. iv). These 14 principles are listed in Appendix A of this document. In July, 2005, The Sedona Conference published *The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production*, as part of their Working Group Series (WG1). This was followed in September, 2005, with *The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age*.

The first of these documents goes into great detail regarding proposed amendments to the Federal Rules of Civil Procedure (FRCP) that are involved with E-discovery. A summary and recap of those rules can be found in Appendix B of this document.

Summary of Amendments

As can be seen in Appendix B, there are several amendments to the Federal Rules of Civil Procedure regarding E-discovery, and they begin with a change in terminology. Federal Rule of Civil Procedure 34, which defines and

gives examples of “documents” and “electronically stored information,” has been updated to include:

... writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any medium from which information can be obtained, translated, if necessary, by the respondent into reasonably usable form” (Shelton, 2006, p. 326).

E-discovery “broadens the scope of examination by including the potential of restoring ‘deleted’ files that may present greater value and relevance in supporting a case position ... [and] In the absence of formal digital document retention and destruction policies and procedures, the [enterprise] is in grave risk of having a Pandora’s Box of damaging data ripe for the taking ” (Guinaugh, 2003, pp. 2-3). One of the most important of the amendments, the effects of this Rule have resulted in a veritable sea change in the ways in which requesting parties are conducting their inquires in the discovery process.

General provisions. The first group of proposed amendments deals with the general provisions which govern discovery, including: the duty of disclosure, required disclosures, and methods of discovery (Court Rules, 2006). They begin with the need to give attention to electronic discovery early in the litigation process. According to Rule 26, “each company has the duty to preserve documents that may be relevant in a case [Scheidlin and Rabkin, 2002a]. This duty to preserve is fundamental to, and inseparable from, the duty of disclosure” (Volonino, 2003, p. 459). Under Rule 26(a)(1)(B), a party must “without awaiting a discovery request, provide to other parties a copy of, or description by category and location of, electronically stored information” (Court Rules, 2006); and under Rule 26(f), “[a] sweeping requirement obliges the company being sued to cite all storage systems

that hold data relevant to the litigation, all relevant data sources and data formats, and the steps counsel has taken to prevent relevant data from being deleted” (Schwartz, 2006, p. 30). Furthermore, Rule 26(b)(1) “enables parties to ‘obtain discovery regarding any matter, not privileged, which is relevant to the subject matter involved in the pending litigation,’ even if the information sought is not admissible at trial” (Gassler, 2002, p. 513). It should also be noted that Rule 26 applies to both parties, and “requires both parties to disclose all information that is relevant to either their claim or defense ... If pertinent data is not disclosed up front, it may not be admissible later” (Schwartz, 2006, p. 32).

The amendments to Rule 26 allow for a “two-tiered process” for production of electronically stored information, the first being accessible data that is stored in the normal course of business; the second being data that is less accessible or which might create an undue burden or cost on the defendant / producing party. This latter category will be subject to further review by the courts with regards to both whether production will be compelled, and which party or parties will bear the cost of such production.

To summarize the General Provisions:

- Duty of disclosure – essentially, every party to the litigation must provide a copy of, or description by category and location of, electronically stored information.
- Required disclosures – regarding any matter, not privileged, which is relevant – even if the information will not be admissible at trial.
- All relevant storage systems and data sources – the party being sued must cite all storage systems and all relevant data sources and data formats, and the steps counsel has taken to prevent relevant data from being deleted or destroyed. [N.B.: Counsel must also sign a document certifying that what they are providing is complete and accurate.]

- A “two-tiered” process – this involves the distinction between what is considered accessible data and less accessible data. Landmark cases have gone on to further define the two (Court Rules, 2006, Lexis/Nexis Applied Discovery ®).

Privileged information and work products. The amendments to Rule 26(f) also cover the issue of documents which fall under the category of “privileged” communication or “work products,” and also seeks to establish some standards regarding what happens in the event of inadvertent delivery of documents that fall into either of those categories. Some of the recommendations in this area include “quick peeks” and/or “clawback” agreements. “It is a good practice to get some kind of agreement early on about privilege issues and present it to the court for incorporation into a case-management order” (Shelton, 2006, p. 328). Further, proposed Rule 34(a) allows a party to request tests or samples of electronically stored information, though “The Committee Note advised that courts should protect parties from ‘undue intrusiveness’ that might arise” (p. 328).

To summarize the amendments regarding privileged information and work products:

- The potential volume of data involved in electronic discovery can be a major challenge, making it nearly impossible to conduct a thorough review of all documents prior to delivery to ensure that privileged information and work product are not inadvertently delivered, as well.
- That being the case, standards were established to deal with this sort of problem, including:
 - quick peeks, and
 - clawback agreements.
- Also allows parties to request tests or samples of ESI, though it does advise that the courts should protect parties from ‘undue’ intrusiveness (Court Rules, 2006, Lexis/Nexis Applied Discovery ®).

Forms of production. FRCP 34(b) goes on to allow the requesting party to specify the format(s) in which the ESI is to be produced, including native format; Tagged Image File (TIF) format; and/or Portable Document Format (PDF). The Rule, however, does not require the producing party to produce in the format requested. Again, it is strongly recommended that this be determined and settled upon during the pre-trial conference to alleviate any misunderstandings or the possibility of having to re-produce the documents.

To summarize, the requesting party can specify the format in which they would like the data delivered, but that request is not binding on the producing party unless so ordered by the Court. Acceptable forms of production include, but are not limited to:

- Native format,
- Tagged Image File format (TIF), and
- Portable Document Format (PDF).

Preservation. Spoliation of evidence refers to the willful destruction of evidence that is germane to the case in litigation. This would include destruction of electronically stored information. However, given the volume of electronic documents created in virtually every business, today, it is usually necessary to delete, archive, and/or overwrite documents in the routine and normal course of business. Accordingly, many companies have data management systems and/or data retention policies in place, which include deletion of electronically stored information on a regular basis.

Preservation of discoverable information is further addressed by Rule 26(f) in terms of the “litigation hold” process. As Judge Scheindlin stated in *Zubulake IV*, “Once a party reasonably anticipates litigation, it must suspend its routine

document retention/destruction policy and put in place a 'litigation hold' to ensure the preservation of relevant documents" (Allman, January/2005, p. 51).

Safe harbor. FRCP 36(f) provides for a safe harbor against sanctions being imposed in the event of electronic information that might be lost under the "routine, good faith operation" of such a data management system or data retention policy. It is important to remember, however, that this amendment does not provide a shield for any party "that intentionally destroys specific information due to its relationship to litigation or for a party that allows such information to be destroyed in order to make it unavailable in discovery by exploiting the routine operation of an information system" (Cortese, 2005, p. 359).

Cost shifting. It is generally understood and accepted that the responding party should bear the cost of production of electronically stored information if the data is "reasonably accessible." If it is not reasonably accessible, however, a cost-shifting analysis will most likely be conducted, as per the precedent set by Judge Shira A. Scheindlin of the U. S. District Court in *Zubulake v. UBS Warburg LLC*. In this landmark case, Judge Scheindlin noted that, "whether production of electronic evidence is unduly burdensome or expensive turns primarily on whether it is kept in an accessible or inaccessible format. And whether electronic data is accessible or inaccessible depends on which of five types of media it is stored on" (Barkett, 2006, p. 335). As further defined in Judge Scheindlin's ruling,

Data which is (1) "online" or archived on current computer systems, such as hard drives, (2) "near-line," such as that stored on optical disks or magnetic tape stored in a robotic storage library from which records can be retrieved in two minutes or less, or (3) "off-line," but in storage or archives, such as removable optical disks or magnetic tape media that are readily accessible using standard search engines because the data are retained in machine readable format.

On the other hand, (4) routine disaster recovery backup tapes that save information in compressed, sequential and non-indexed format, and (5) erased, fragmented or damaged data are generally inaccessible, because a time-consuming, expensive restoration process is required to obtain the information (p. 335).

Judge Scheindlin went on to craft a three-step analysis process to be considered in the cost-shifting decision. In the first step, it is necessary that the Court be knowledgeable about the responding party's computer system to be able to assess whether the data is or is not accessible. "Second, since the 'cost shifting analysis is so fact-intensive, it is necessary to determine what data may be found on the inaccessible media' " (Barkett, 2006, p. 336). And finally, Judge Scheindlin concluded that seven factors should be considered in making the final determination:

1. The extent to which the request is specifically tailored to discover relevant information.
2. The availability of such information from other sources.
3. The total cost of production, compared with the amount in controversy.
4. The total cost of production compared to the resources available to each party.
5. The relative ability of each party to control costs and its incentive to do so.
6. The importance of the issues at stake in the litigation.
7. The relative benefits to the parties of obtaining the information (Barkett, 2006, p. 336).

The corresponding amendments to Federal Rule 37 have adopted and continue to follow these guidelines. It should be noted here, however, that "Rule 37 in no way suggests that cost sharing should be considered with regard to the preservation of electronically stored information ... [though] The Committee Notes accompanying Rule 26(b)(2) ... hint that cost allocation can be considered in

circumstances requiring extraordinary production of such information” (Rice, Sterchi, and Boschert, 2006, p. 172).

Landmark Cases

Landmark cases are certainly important in and of themselves, particularly to the litigants involved. But they are even more important in the fact that they pave the way and set the precedents that will usually be followed in the course of future litigation. In cases involving electronic discovery, this was true even prior to the enactments of the amendments to the Federal Rules of Civil Procedure. The case of *Zubulake vs. UBS Warburg, LLC*, for example, began in 2002.

Zubulake vs. UBS Warburg, LLC. Arguably the most noteworthy landmark case can be considered to be *Zubulake vs. UBS Warburg, LLC*. This was a gender discrimination case, which “concluded with a federal jury mandate that UBS pay \$20.2 million in damages. ... The case is significant because of several rulings made as the trial progressed – rulings that put the burden of producing electronic evidence squarely on the shoulders of the companies issued with discovery and created precedents of penalties for failure to adequately do so” (Murphy, 2005). The *Zubulake* case “also confirmed the rule ... that ordinary negligence is a sufficiently ‘culpable state of mind’ to support an adverse inference” (Sedor, 2006, p. 3).

It is important to note that *Zubulake* continues to provide us with precedent setting opinions that all attorneys should be familiar with.

Zubulake V represents the first time that a court has set forth such explicit guidelines for attorneys managing the preservation and production of electronic evidence. The betting money is that courts will largely fall in like dominoes behind the principles of *Zubulake* with only minor modifications. If this is true, the waters will no

longer be uncharted and navigation by legal counsel must be considerably more zealous and comprehensive than it has been in the past. If you ignore *Zubulake V*, you risk being scorched by a dragon's breath as you flounder in perilous waters (Nelson and Simek, 2005, p. 23).

"As a sidebar note, since *Zubulake V* came down, the American Bar Association's standards have been revised to offer an updated and more pragmatic approach to preservation of evidence and production obligations. The amendments may be found at

<http://www.abanet.org/litigation/documents/home.html> " (Nelson and Simek, 2005, p. 23).

Rowe Entertainment v. William Morris Agency. This involved a \$600 million antitrust case in which black concert promoters contended that they had been "frozen out of the market for promoting events with white bands" (Lexis/Nexis, 2005). The real point to this case was in the nature of the costs involved in full delivery of all potentially pertinent electronic data. The defendants in this case strongly contested the issue of the costs involved, estimating the cost at \$395,944 if eight selected backup sessions were produced, and as much as \$9,750,000 if tapes of all backup sessions were required to be produced.

United States v. Philip Morris USA, Inc. This case alleged that Philip Morris had "actively targeted youth through marketing and advertising campaigns, manipulated the nicotine content of its cigarettes to make and keep smokers addicted, and failed to market potentially less hazardous cigarettes" (Scheidlin and Wangkao, 2005). In this case, Philip Morris continued deleting emails for two years after the Court issued a preservation order, and in fact, after learning of its inadequate preservation efforts, continued deleting emails for an additional two

months and neglected to notify the courts and the government of the deletions for yet an additional four months. They were ultimately charged \$2.75 million in fines for spoliation of data since “Philip Morris had shown a ‘reckless disregard’ toward its discovery obligations” (Scheindlin and Wangkao, 2005).

Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc. “In perhaps the most infamous e-discovery sanctions case to date, CPH sued financial giant Morgan Stanley for fraud in connection with CPH’s sale of stock” (Sedor, 2006, p. 1). In the course of this case, CPH sought access to Morgan Stanley’s internal emails. “Morgan Stanley partially complied, but its internal team in charge of the project knowingly failed to search many hundreds of backup tapes and falsely certified the production as complete. Morgan Stanley then notified CPH and the Court that there were thousands of additional responsive e-mails and that the team was continuing to find additional backup tapes, and was still searching ... for more e-mails just a month before trial. To make matters worse, Morgan Stanley’s counsel misrepresented facts relating to when the team had found the backup tapes and equivocated about the timeframe for completion of the searches” (Sedor, 2006, p. 2).

The judge issued an adverse inference order, “which allows the jury to infer that the spoliator destroyed evidence because it knew it was unfavorable, often cannot be overcome, and forces an end to litigation” (Sedor, 2006, p. 2). To make matters worse, “the court learned that the company had intentionally hidden information about its discovery violations and had “coached witnesses not to mention” the additional backup tapes (Sedor, 2006, p. 2).

Since it was found that further searches of backup tapes could not be performed in time for trial, "the court catalogued the ample evidence of willful and grossly negligent misconduct," entered a default judgment against Morgan Stanley, "and deemed the majority of CPH's complaint established" (Sedor, 2006, p. 2) in this record setting \$1.45 billion dollar settlement, which included over \$604 million in compensatory damages and \$850 million in punitive damages.

American Home Products. American Home Products (AHP) are the manufacturers and distributors of the anti-obesity medication, Fen-Phen, a combination of fenfluramine and phentermine. In this case, internal email of defendant AHP was subpoenaed, resulting in a search of more than 33 million emails. "Plaintiffs' computer forensics experts uncovered e-mail stating:

'Do I have to look forward to spending my waning years writing checks to fat people worried about a silly lung problem? [Keena, 2002]'

American Home Products was charged with reckless indifference to human life, and settled the case for a record \$3.75 billion" (Volonino, 2003, p. 461).

Implications for Business

In their section titled, "Federal and State Court Rulings on E-Discovery and Computer Forensics," Cyber Controls, LLC, a cyber forensics support services firm, noted that in 2002 alone, more than 265,000 federal cases were filed wherein approximately 5,000 cases included "significant levels of electronic discovery" (2008, ¶1). Appendix E of this document provides a summary listing of their categories of case law review, which includes cases involving the following:

- Scope of E-Discovery;
- Forms of Electronic Discovery;
- Computer Forensic Protocols;

- Records Management;
- Forms of Production;
- Procedure;
- Production of Data;
- Privacy & Privilege;
- Spoliation;
- Data Preservation & Spoliation;
- Sanctions;
- Employee Email;
- Discovery of E-Evidence Denied;
- Admissibility; and
- Costs.

A number of cases are listed under each of these categories. The authors also note this list of case law reviews is ever growing.

Two areas of particular concern come in the form of IMs and e-mails, particularly due to the trend of their rapidly increasing use. “With e-mail and IM sources of e-evidence, companies are [even more] exposed to risks of liability and litigation because:

- Casual, private or seemingly irrelevant e-mail messages or IM may be deemed business records, which even strongly worded disclaimers cannot repudiate.
- Communications made in confidence are not protected from disclosure if they fit the legal definition of business records.
- E-mail or IM that did not meet the definition of business records when they were created might nevertheless be required as evidence in court. For example, an administrative e-mail notice of a company softball game could be used as evidence in a workers’ compensation claim if an employee is injured during the game [Flynn and Kahn, 2003]” (Volonino, 2003, p. 458).

There is also a clear indication that many roles will be changing. The changes brought about by the new E-discovery Rules will affect “every business,

organization and person that may ever be involved in a federal court case” (Curtis, 2006, p. 1). And sooner or later, that will involve nearly every business organization, in one way or another. Chief Information Officers (CIOs), risk managers, and legal counsel will need to work together in ways they never have before this. As Michael Gold, senior partner with Jeffer Mangels Butler & Marmaro noted, “ ‘It’s a corporate cultural change, and it will take a fair amount of time to work out’ ” (Sloat, 2006).

In their book, *From Business Strategy to IT Action*, Benson, Bugnitz, and Walton noted the growing importance of IT’s involvement in the strategic planning process and the frequent disconnects in this area. Perpetuating the silos that exist between business and IT will no longer be an option. “Culture predefines IT’s role in the business, and limits what and how IT can contribute” (Benson, Bugnitz, and Walton, 2004, p. 214). It has become more important than ever that top management examine that culture and assess these relationships in a new light.

It is important that we all “[k]eep in mind that, in the knowledge economy, everyone is his or her own records custodian” (Spira, 2007, p. 3). Most of us give only our passing attention to those e-mails that come from IT with regards to policies and procedures that relate to record retention compliance. “The reality is that it is often worse to have a document retention policy that is not followed – or followed in an inconsistent fashion – than no policy at all” (Boehning and Twiste, 2006, p. 58).

Without a doubt, “the discovery of e-evidence [has] assumed enormous importance in litigation. As regulatory agencies intensify investigation of corporate malfeasance and computer crimes, the obligations imposed on companies and

their staff[s] increases correspondingly” (Volonino, 2003, p. 461). When we combine the growing volume of electronic data with the growing number of cases, along with the skyrocketing costs of litigation and the severity of sanctions imposed for non-compliance, there is little question that the new amendments to the Federal Rules of Civil Procedure have had, and will continue to have, a major impact on risk to the enterprise.

Chapter III

METHODOLOGY

As Cooper and Schindler note, “Research design is the plan and structure of investigation so conceived as to obtain answers to research questions” (2003, p. 146). It is “the blueprint for fulfilling objectives and answering questions” (p. 81). Thus, in determining the methodology that will be used in the course of research, it is important to first understand the purpose of that research and to determine what those objectives and questions are. In other words, “the coverage of the design must be adapted to the purpose” (p. 663). Maxwell further substantiates this, as he notes, “Your research questions – what you specifically want to understand by doing your study – are at the heart of your research design. ... More than any other aspect of your design, your research questions will have an influence on and should be responsive to, every other part of your study” (2005, p. 65).

Research Objectives

The objective of this research study is to investigate the level of awareness of organizations regarding the Federal Rules of Civil Procedure (FRCP) that were enacted into legislation on December 1, 2006, and their current level of preparedness for the eventuality of litigation involving electronic discovery (E-discovery). Details of the Rules and the amendments thereto will be discussed, as well as their potential impact on enterprise risk. The study will also explore the relationship between the level of awareness of the FRCP and the organization’s level of preparedness.

Research Questions

In light of the fact that the new FRCP were enacted into law on December 1, 2006, to date, there has been very little research published with regards to organizations' levels of awareness of, and preparedness for, the potential impact of the Rules in the event of litigation involving E-discovery. Absent existing published research, this study will be exploratory in nature. At this point in the study, the research question is general in nature:

- What is the level of awareness of the newly enacted amendments to the Federal Rules of Civil Procedure within and among the various functional areas of the enterprise?

Subordinate facets to the primary research question include the following questions, as well:

- What is the level of awareness of the potential impact of the new amendments to the Rules on enterprise risk?
- How well prepared is the organization to comply with the new amendments to the Rules?

In summary, the more we learn about the level of awareness that exists at various levels of the enterprise, and the relationship between awareness and the potential impact of that awareness on organizational policies and actions, the better equipped we will be to provide the tools needed to manage its risks.

Qualitative Research

“The objectives of exploration may be accomplished with different techniques. ... although exploration relies more heavily on qualitative techniques”

(Cooper and Schindler, 2003, p. 151). As such, this research study will be based on qualitative research methods. According to Creswell (2005),

Qualitative research is a type of ... research in which the researcher relies on the views of participants, asks broad, general questions, collects data consisting largely of words (or text) from participants, describes and analyzes these words for themes, and conducts the inquiry in a subjective, biased manner (p. 39).

Characteristics of qualitative research include:

- a recognition that as researchers we need to listen to the views of the participants in our studies,
- a recognition that we need to ask general, open questions and collect data in places where people live and work, and
- a recognition that research has a role in advocating for change and bettering the lives of individuals (Cresswell, 2005, p. 43).

The central phenomenon of this qualitative research turns on the awareness and preparedness of organizations to deal with the requirements of electronic discovery in the event of litigation. As qualitative research seeks “to learn more from participants through exploration” (Cresswell, 2005, p. 45), this study seeks to learn more about the processes of awareness and preparedness as they relate to the potential impact of electronic discovery under the requirements of the amended Federal Rules of Civil Procedure.

This research study will also have elements of action research. “Action research designs are systematic procedures ... to gather quantitative and qualitative data to address improvements ... [and] seek to address and solve local, practical problems” (Cresswell, 2005, p. 53). As we assess the levels of awareness and preparedness for E-discovery, and come to better understand the processes of awareness and preparedness, we will be better able to mitigate the negative impact of E-discovery on enterprise risk.

Justification for the Research

Cresswell (2005, p. 64) notes five ways to assess whether a particular problem or phenomenon should be researched, four of which are addressed in this research study as follows.

Study the problem if your study:

1. *will fill a gap or void in the existing literature.*

E-discovery is a new area of study, for which not much research has been conducted and published, to date.

2. *replicates a past study, but examines different participants and different research sites.*

A quantitative pilot study has been conducted on a limited scale, which data is available for comparative analysis.

3. *study extends past research or examines the topic more thoroughly.*

This study will add qualitative data that may bring new perspectives to the field for further study.

4. *informs practice.*

This study will help create a new level of awareness among various levels of management that are affected by E-discovery.

The Research Plan

According to Miles and Huberman, "The researcher's role is to gain a 'holistic' (systemic, encompassing, integrated) overview of the context under study: its logic, its arrangements, its explicit and implicit rules. ... [In the course of this effort,] the researcher attempts to capture data on the perceptions of local actors 'from the inside' " (1994, p. 6). They go on to note that, "A main task is to

explicate the ways people in particular settings come to understand, account for, take action, and otherwise manage their day-to-day situations” (p. 7).

The process flow diagram for this proposed research model can be found in Appendix D of this document. As noted therein, this study will consist of a set of interviews with experts in various functional areas of their respective organizations, such areas include, but are not limited to finance, accounting, legal, and human resources. Where possible, the participants will represent different industries and different levels within the organizational hierarchy. The interviews will incorporate both structured and unstructured questions. At the conclusion of each interview, the participant will be asked to complete a survey instrument that was previously used in a pilot test. This survey instrument can be found in Appendix F.

The purpose of this request is twofold: first, the study seeks to determine how closely the responses correlate to those of the original pilot study; and the study seeks to validate the survey instrument for potential future use on a broader scale. Second, respondents will be asked for their perspective on each of the questions presented, regarding its relevance in terms of both their position within their organization, and in terms of its relevance to the organization itself. They will also be asked whether there are other questions they feel would be appropriate from the perspective of their particular functional area(s) of the business.

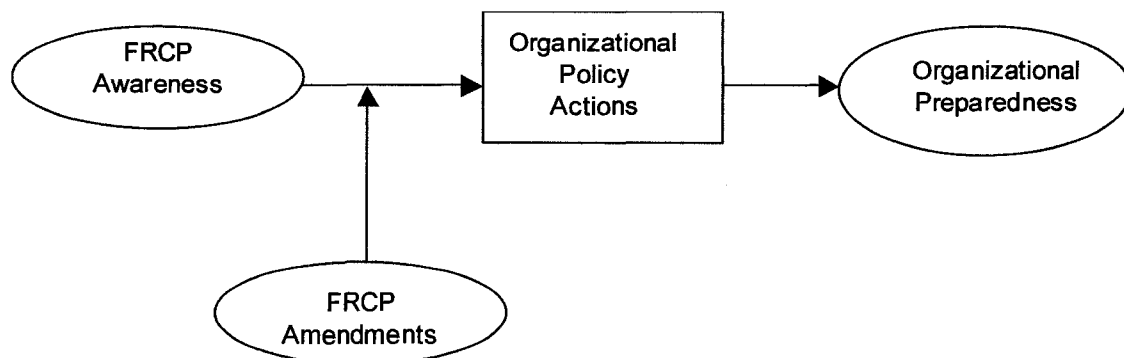
Interviews will be conducted face-to-face, with an expected duration of between 30 and 60 minutes, and will be tape-recorded. Each potential participant will be provided with a general consent form detailing the purpose of the research. The consent form also advises the potential participant that taking part in the project is entirely voluntary, and further notes that the participant may elect to

decline and / or withdraw from the study at any time, and without penalty. A second consent form requests permission from the participant to tape-record the interview. The Audio/Videotape Consent form also provides the participant with the opportunity to hear the tapes before they are used for this research project, thus providing a second opportunity to elect to withdraw his or her participation in the project. These consent forms may be found as Appendixes H and I, respectively. All possible efforts will be taken to ensure the privacy of both the participants and their organizations.

Purposeful selection was used to determine the list of participants selected. As noted in Maxwell (2005), purposeful sampling "is a strategy in which particular settings, persons, or activities are selected deliberately in order to provide information that can't be gotten as well from other choices" (p. 88). In this case, the participants were selected due to their varied functional areas of expertise and the variety of industries their organizations represent. Requests for participation will be made at the personal behest of the researcher. Maxwell further notes a potential goal of purposeful selection "can be to establish particular comparisons to illuminate the reasons for differences between settings or individuals" (2005, p. 90). This study seeks to illuminate the potential reasons for differences in awareness and preparedness among different functional areas of the enterprise in an effort to achieve multi-disciplinary perspectives, as the study also seeks to understand if there are variations in level of awareness by functional area of the business enterprise.

The conceptual framework for this research will be based in grounded theory. Grounded theory "does not refer to any particular *level* of theory, but to

theory that is inductively developed during a study ... and in constant interaction with the data from that study. This theory is 'grounded' in the actual data collected" (Maxwell, 2005, pp. 42-43). "Grounded theory inquiry is portrayed as a problem-solving endeavor concerned with understanding action from the perspective of the human agent" (Haig, 1995, ¶ 2). A goal of this research is to develop a theory that will allow the researcher to better understand the relationships that exist between awareness of the Federal Rules of Civil Procedure (FRCP), the recently enacted amendments to the FRCP, organizational policy actions, and organizations' preparedness to comply with the FRCP in the event of litigation involving electronic discovery, as can be seen below.



This concept flow diagram depicts the questions this research is seeking to answer:

- What is the general level of awareness regarding the Federal Rules of Civil Procedure?
- What is the level of awareness regarding the recently enacted amendments to the Federal Rules of Civil Procedure and their potential impact on risk to the enterprise?

- How do these levels of awareness affect the organization's policy decisions?
- What impact does all this have on the organization's level of preparedness in the event of litigation involving electronic discovery?

As Miles and Huberman note, "We have to face the fact that numbers and words are *both* needed if we are to understand the world" (1994, p. 40). The ultimate goal of this research study is the integration of the data collected from the pilot study and the data collected from the interviews. The results of this integration will assist the researcher in determining the merit of further quantitative study, expanding on the original pilot cyber forensic study, as well as its direction and focus.

Potential Validity Concerns

Potential validity concerns begin with the nature of the participants selected for interviews. Participants will be selected by convenience and based on their personal relationship with the researcher. Based on this relationship, and the fact that the researcher is well acquainted with the participants, both the nature and identity of the participant's organization are known to the researcher. As a result, the participants may be reticent about revealing full and complete information regarding their organizations.

According to Marshall and Rossman, "an assumption fundamental to qualitative research [is that]: the participant's perspective on the phenomenon of interest should unfold as the participant views it, not as the researcher views it" (1995, p. 80). A second validity concern is the researcher's potential bias on this topic. Based on much of the literary research conducted thus far, as well as the

nature of the interviews, it will be imperative to set preconceived expectations aside as the research is conducted and analyzed.

A third validity concern is inherent in the nature of interviews, in general. While interviews provide us with the means to gather useful data, there is no real way to ensure that the data being gathered is, in fact, factual and accurate. In an effort to appear to be cooperative, the possibility always exists that the participant will provide the response he or she feels the researcher wants to hear. This is particularly true in the case where the researcher and the participant have a prior relationship. It will be very important for the researcher to ensure the participant does not feel pressured to participate, for any reason. By reducing or eliminating any perception of pressure to participate, the responses received are expected to be more spontaneous and genuinely representative of the participant's level of awareness of the new amendments to the FRCP and their potential impact to the participant's organization.

Human Subjects Statement

In any kind of research involving human subjects, the researcher has the ethical responsibility to ensure that any and all participants suffer no harm. As previously noted, requests for participation in this research will be made at the personal behest of the primary researcher, and is strictly voluntary. Confidentiality and anonymity will be maintained at all times. Potential participants / interviewees will be provided with both a general consent form and a consent for the audio taping of the interview sessions. Specifically, the consent form notes:

If you choose to take part in this project, you will be helping provide valuable information toward future research in this area, and will also gain additional

insight and information regarding the newly enacted legislation that may be of benefit to you and your organization. Taking part in this project is entirely voluntary and no one will hold it against you if you decide not to participate. If you do decide to participate, you may stop at any time without penalty. In addition, you may ask to have your data withdrawn from the study after the research has been conducted.

The audiotape consent form requests the participant's permission to tape-record the interview and further requests permission to use the tapes for the purpose of the research project. The consent form also provides the participant with the opportunity to hear the tapes prior to making the final decision to allow their use.

In summary, the consent forms:

- Provide for informed consent;
- State unequivocally that participation is strictly voluntary; and
- Provide for the right of withdrawal at various points in the research process.

Chapter IV

FINDINGS

As noted in Chapter III, the objective of this research study is to investigate the level of awareness of organizations regarding the amendments to the Federal Rules of Civil Procedure (FRCP) that were enacted into legislation on December 1, 2006, the ultimate effects of that awareness on the organizations' policy actions, and the resultant level of organizational preparedness in the event of litigation involving electronic discovery. The goal of the researcher is to gain a better understanding of the process that leads from awareness to preparedness in order to develop a better conceptual framework for further study. The current framework of grounded theory allows the researcher to gain a holistic perspective of this process, and to help "explicate the ways people in particular settings come to understand, account for, take action, and otherwise manage their day-to-day situations" (Miles and Huberman, 1994, p. 7).

The focus of this study is to investigate how the level of awareness of organizations regarding the Federal Rules of Civil Procedure and the amendments thereto affect organizational policy actions that ultimately result in organizational preparedness for the eventuality of litigation involving electronic discovery. This was accomplished by attempting "to capture data on the perceptions of local actors 'from the inside' " (Miles and Huberman, 1994, p. 6) who are deemed to be experts in their respective functional areas of finance, accounting, human resources, et cetera.

Data Collection

Data collection methods included face-to-face, audiotaped interviews around an agenda consisting of both structured and unstructured questions. A standard interview agenda consisting of 18 questions was used. The general consent form, the consent form for audiotaping the interview and the interview agenda can be found in Appendixes H, I, and J, respectively. The questions focused on general awareness of the Federal Rules of Civil Procedure (the “Rules”), the recently enacted amendments to those Rules, how the Rules might apply to the organization in question, and how the Rules might apply to the role of the interviewee, in particular.

Also included as part of the interview process was the completion of a cyber-forensic survey instrument that was previously used in a pilot test, and which can be found in Appendix F. Completion of the survey was requested for the following purposes:

- to compare the results against those of the original pilot study;
- to seek input regarding the interviewee’s perception of the appropriateness of the survey and the questions posed therein; and
- to validate the survey instrument for potential future research.

The survey was willingly completed by the interview subject in all interviews.

In the course of purposeful selection, it is often difficult to gain access to appropriate interview subjects. They are typically high profile individuals with busy schedules, which are subject to change. This challenge was only exacerbated by the fact that the research was conducted over the summer months when vacations

and cross coverage for the absence of others in the organization only served to add to the challenges of time and availability.

The researcher initially contacted twenty individuals with the request for an interview, and all responded affirmatively. Four of those candidates were unable to keep their original appointments with the researcher; two requested rescheduling, but were still unable to make our appointments and participate. In an effort to ensure the participants in question did not feel pressured or compelled to participate, or to participate with less than full candor, requests to participate were not repeated.

The interviews conducted involved companies in different industries, represented by individuals in varying levels of management positions, and in various functional areas of the business. As noted in Table 1 on the following page, this included but was not limited to a Corporate Controller, a Director of Finance, an Internal Auditor, and a Senior Vice President of Human Resources; representing publicly held, privately held, municipal government, and not-for-profit organizations. The same interview agenda was followed with each participant, though in some cases additional discussion ensued based on the initial responses received. With consent of the interviewee, each interview was tape-recorded, and each interviewee was offered the opportunity to review the recording at his or her convenience. All but one interviewee declined the option to review his or her audiotape. In order to preserve the confidentiality of the participants, their names have been replaced in Table 1 with identifiers labeled as Interviewee P-01, P-02, P-03, et cetera, and their company names have been replaced with industry

identifiers, followed by legal status of the organizational entity (i.e., publicly held corporation, privately held corporation, Limited Liability Company (LLC), et cetera).

Table 1 – List of Interviewees

Interviewee	Title	Industry	Org Type
P-01	Controller	Construction	Privately held corporation
P-02	Internal Auditor	Transportation	Publicly held corporation
P-03	VP - Human Resources	Food Supplier	Publicly held corporation
P-04	Finance Director	Municipality	Municipal Government / Not for profit
P-05	General Manager	Manufacturing	Privately held corporation
P-06	Executive Vice President	Engineering / Design	Privately held corporation
P-07	Owner / Hospital Administrator	Medical Services	Privately held LLC
P-08	Owner / Consultant	HR Consulting	Privately held corporation
P-09	Managing Director	Financial Services	Publicly held corporation
P-10	Attorney / External Counsel	Legal Services	Privately held LLC
P-11	Sole Proprietor / Management Consultant	Consulting Services	Sole proprietorship
P-12	Information Systems Analyst	Publishing	Publicly held corporation
P-13	Instructional Designer	Financial Services	Publicly held corporation
P-14	President / Sole Proprietor	Consulting Services / Financial & Healthcare	Sole proprietorship
P-15	Owner / Sole Proprietor	Consulting Services / Technology & Networking	Sole proprietorship
P-16	Regional Team Lead	Consulting Services / Manufacturing (Ops Mgt)	Privately held / Not for profit

Summary of Interviews

The interviews began by asking the interviewees about their familiarity with various laws and regulations regarding data retention, then moved on to ask if they were at all familiar with the Federal Rules of Civil Procedure, in general terms. Interview questions 2, 3 and 4 were directly related to the primary research question.

Table 2

Interview Responses Relevant to Primary Research Question

What is the level of awareness of the newly enacted amendments to the Federal Rules of Civil Procedure (FRCP) within and among the various functional areas of the business?

Q2: Are you aware of any of the various laws and regulations regarding data retention?

P-01	Yes	P-05	No	P-09	Yes	P-13	Yes
P-02	Yes	P-06	Yes	P-10	Yes	P-14	Yes
P-03	Yes	P-07	Yes	P-11	Yes	P-15	Yes
P-04	Yes	P-08	Yes	P-12	Yes	P-16	Yes
* Positive responses: 15 out of 16, or 93.75%							

Q3: Do you know anything about the Federal Rules of Civil Procedure – what they are or what they're about?

P-01	No	P-05	Yes	P-09	No	P-13	No
P-02	No	P-06	No	P-10	Yes	P-14	No
P-03	No	P-07	No	P-11	No	P-15	No
P-04	No	P-08	Yes	P-12	No	P-16	No
* Negative responses: 15 out of 16, or 93.75%							

Q4: Do you think these rules might apply to your organization?

P-01	Yes	P-05	Yes	P-09	Yes	P-13	Yes
P-02	Yes	P-06	Yes	P-10	Yes	P-14	Yes
P-03	Yes	P-07	Yes	P-11	Yes	P-15	Yes
P-04	Yes	P-08	Yes	P-12	Yes	P-16	Yes
* Positive responses: 16 out of 16, or 100%							

As can be seen in Table 2 above, in nearly every case (93.75%) the interviewee was aware, at least in general terms, of other legislation relating to data retention requirements including Sarbanes-Oxley (SOX), the requirements of Generally Accepted Accounting Principles (GAAP), Equal Employment Opportunity Commission (EEOC) requirements, the Gramm-Leach-Bliley Act (GLBA), the Occupational Safety and Health Act (OSHA), requirements of the Health Insurance Portability and Accountability Act (HIPAA), and the Patriot Act. Most of the interviewees (81.25%), however, were not familiar with the Federal Rules of Civil Procedure (FRCP), or the amendments thereto (93.75%), enacted into law on December 1, 2006. As can be further seen in Table 2, all interviewees felt the Rules applied to either their own organizations and/or to their clients' organizations.

Interview Questions 6, 7 and 11 directly addressed Subordinate Research Question (1). In each interview, a summary of the Rules was presented, along with a synopsis of the recently enacted amendments. At the conclusion of this discussion, each interviewee was asked how he or she thought those Rules might apply to their organization, and in particular, how they might apply to their own roles and responsibilities in the organization. These results are summarized in Table 3, which follows on the next page. As can be seen in Table 3, 93.75% of all respondents were completely unaware of the amendments to the FRCP and were not familiar with any of those changes. All interviewees, however, felt both the Rules and amendments thereto applied to their organizations, but with varying levels of potential impact.

Table 3**Interview Responses Relevant to Subordinate Research Question (1)*****What is the level of awareness of the impact of the new amendments to the FRC) on enterprise risk?***

Q6: Are you aware of any of the fact that a number of amendments and changes to these Rules went into effect December 1, 2006?

P-01	No	P-05	No	P-09	No	P-13	No
P-02	No	P-06	No	P-10	Yes	P-14	No
P-03	No	P-07	No	P-11	No	P-15	No
P-04	No	P-08	No	P-12	No	P-16	No
* Negative responses: 15 out of 16, or 93.75%							

Q7: Are you familiar with any of those changes?

P-01	No	P-05	N	P-09	No	P-13	No
P-02	No	P-06	N	P-10	Yes	P-14	No
P-03	No	P-07	N	P-11	No	P-15	No
P-04	No	P-08	N	P-12	No	P-16	No
* Negative responses: 15 out of 16, or 93.75%							

Q11: Do you think these Rules pose any new risk to your organization?

P-01	Yes	P-05	Yes	P-09	No	P-13	No
P-02	Yes	P-06	No	P-10	Yes	P-14	Yes
P-03	No	P-07	Yes	P-11	Yes	P-15	Yes
P-04	Yes	P-08	Yes	P-12	No	P-16	Yes
* Positive responses: 11 out of 16, or 68.75%							

The perceived range of impact seemed to be linked to the size of the organization and the “depth of its pockets,” as well as to the industry (e.g., financial institutions and governmental organizations are traditionally more conservative in nature, and thus more inclined to standardization and retention of documentation), or the nature of the organization (i.e., public, private, municipal; for profit, not-for-

profit). Another strong factor on perceived impact involved whether or not the firm had previously been involved in litigation.

Based on the results of the interviews, and given the fact that 93.75% of the interviewees were not even aware of the Federal Rules of Civil Procedure, much less the amendments thereto, it is clear that there was little awareness of the amendments within and among the various functional areas of the business organizations that are represented in this research. It is also clear that there was little to no awareness among the participants represented herein regarding what the new amendments mean in terms of impact on enterprise risk.

How the Rules and amendments might apply to the interviewee's role and responsibility varied in direct relation to those roles and responsibilities. Two of the interviewees have responsibility for human resources (HR) functions within their organizations, the Vice President of HR and the Corporate Controller; two additional interviewees provide HR services and consultancy to their clients' organizations. In each of those cases, the interviewee noted responsibility for all employment related issues and documents. In the case of Interviewee P-03, it was further noted that most charges filed named both the company and the individual as co-defendants in employment-related litigation – which involved approximately 80% of all litigation that organization was involved in. Interviewee P-02 felt there was stronger applicability in the case of auditors based on the fact that they are responsible for monitoring and reporting on any irregularities that may exist in the organization, and may be called as witnesses in litigation. It was interesting to note that interviewee P-08 had a very different perspective, noting that HR personnel are frequently called upon to testify, since most cases involve

termination and / or other personnel-related cases, and pointedly remarked that “auditors and the like” were much less aware because they seldom found themselves “in the hot seat” of having to testify in the event of litigation.

Interviewee P-04 felt there was little direct impact on that particular role in the organization, save for the possible eventuality of having to come up with the financial resources for settlement. Interviewee P-05 noted the need to be more sensitive and more aware of what data was being kept, for how long, and ensuring full compliance with both their data retention and their data destruction policies. As the owner / administrator responsible for a medical services business, interviewee P-07 felt that with the new awareness came the need to write and implement formal policies as soon as possible, as well as for providing more formal, regularly scheduled, and more rigorous audits of those policies. Interviewee P-09 noted that their organization often works in a multi-level team structure, wherein non-public client information is provided to members who process and run reports against that data. This individual also noted lack of awareness regarding what was done with the data after it was passed on – i.e., whether it was filed for future reference, destroyed for security purposes once the report was provided to management, or otherwise handled or distributed. This interviewee went on to add that more formal policies and procedures in this area are probably warranted, with tighter controls in place.

As an Instructional Design Specialist, interviewee P-13 noted that training materials are often developed using actual data in an effort to provide more realistic and recognizable examples to their trainees. This individual noted the need to be more aware of the nature of the data being used as the basis for those

training materials, as well as a greater awareness of all the components of *what* needs to be trained on, including data management and data handling.

Interviewees who were in consultancy roles felt the greatest impact would not be in the form of their roles within their own organizations, but in the roles they played in the clients' organizations. In each of these cases, they felt their role was more impacted by the need to ensure their clients were made aware of the FRCP and the new amendments, and the potential impact those amendments might have on the enterprise risk of their *clients'* organizations. This meant not only becoming more knowledgeable regarding the Rules and the amendments themselves, but also becoming more knowledgeable regarding expert resources available to their clients that could better assess the risks involved and provide custom tailored services to meet each client's needs in this area. A few individuals in this area also noted that this could potentially open up an entirely new area of consultancy and advisement for their organizations.

Next, the interviewees were asked what kind of impact they felt the Rules might have on their organizations, and whether they felt the Rules posed any *new* risks. Most noted that there would be an impact on any current or future litigation. The new risks that were noted included the need for additional training at all levels of the organization, and in particular, the need for training and awareness among all management levels of the organization; the trend of employees to co-mingle personal and business communications and data; and potential risk to employees of being included in the discovery process on a personal level. In general, the interviewees seemed to feel the greatest impact came not so much from the Rules and the new amendments, but rather, from the increase in the volume of data and

use of company resources by a greater number of employees who might be unfamiliar with the impact of their actions – notably, the co-mingling of personal and business data – and the fact that it is becoming increasingly difficult, if not impossible, to be completely aware of every piece of data or communication that is occurring via the use of organizational resources (i.e., e-mail, e-mail attachments, phone systems, peripheral storage devices, et cetera).

The final question on the interview survey was directly related to Subordinate Research Question (2). Responses to this question were more varied.

Table 4

Interview Responses Relevant to Subordinate Research Question (2)

How well prepared is the organization to comply with the new Amendments to the FRCP?

Q13: In the event of litigation, do you think your organization is prepared to comply with these new Rules?

P-01	No	P-05	Yes	P-09	Yes	P-13	Yes
P-02	No	P-06	Yes	P-10	Yes/No	P-14	Yes/No
P-03	Yes	P-07	Yes	P-11	Yes/No	P-15	Yes
P-04	Yes	P-08	Yes/No	P-12	Yes	P-16	Yes
* Positive responses:		10 out of 16, or 62.5%					
* Yes/No responses:		4 out of 16, or 25.0%					
* Negative responses:		2 out of 16, or 12.5%					

As can be seen in Table 4 above, 62.5% of interviewees felt their organizations were prepared to comply with the new amendments to the FRCP; 25% felt their organizations were probably prepared to comply but were not sure; and 12.5 % of respondents felt their organizations were not prepared to comply. Responses included comments such as the following:

Survey Question 13: In the event of litigation, do you think your organization is prepared to comply with these new rules? Why / why not?

- Interviewee P-01: Effectively, no. We're a small firm and tend to be reactive rather than proactive.
- Interviewee P-02: I don't know, but they won't have much choice in the matter.
- Interviewee P-03: Absolutely. Based on SOX, EEOC, and other regulatory requirements – and previous litigation – we know without question where everything is and how to access it.
- Interviewee P-04 (with a laugh): Probably yes, because we also tend to keep paper copies of everything, with most of it being available as far as 30 years back.
- Interviewee P-05: Yes. As I previously noted, we have only a limited number of sites and hardware where the information is stored, with a closed-loop system out of only one facility.
- Interviewee P-06: Yes – our industry has moved very slowly in terms of technology, and we haven't been dealing with entering everything electronically until the last couple of years.
- Interviewee P-07: Yes – we're small and don't have many layers. Since I keep and maintain all records, I could probably do it pretty quickly at this point. On the other hand, if we grow to a multi-state level, as we hope to do, we'll have to make sure we keep these things in mind in our planning.
- Interviewee P-08: Absolutely – I'm ready to comply because I've been there, so I know what I need to do.
- Interviewee P-09: I don't really know – but probably, since we've had to go to court before.

- Interviewee P-10: As for our firm, yes; as for our clients, we had a seminar on this topic so probably yes, but in general, I can't say for sure.
- Interviewee P-11: Today, probably not fully; but to some degree, yes, because of the other laws that are in effect regarding data retention and data management.
- Interviewee P-12: Yes, I really do. We've been pretty proactive with audits and making sure we're all compliant with these types of policies.
- Interviewee P-13: Oh yes. Business continuity plans are in place, and we have a well-defined, redundant network. Plans are in place and we're very aware of what is stored, and where. This is very important in light of what we do regarding trades on customer accounts, et cetera.
- Interviewee P-14: In my own case, yes. In the case of my clients, no I don't think so. I don't really focus on that area, but you've given me some food for thought to share with some of the CEOs I deal with.
- Interviewee P-15: Yes, I do, because we're limited in storage devices and storage space. So what we have, and where it is, is fairly limited. Data backups are all catalogued and well organized.
- Interviewee P-16: Yes. We only have a handful of laptops available, and if we received a notice we'd immediately confiscate the machine(s) involved and turn it/them over.

At the conclusion of the interview, each participant was asked if they felt the questions were appropriate to the topic at hand (cyber-forensic preparedness), and if they felt it was appropriate for their organization. Each interviewee responded affirmatively. They were then asked if they could think of additional questions that might be appropriate, or helpful to them in their roles in their organizations.

Interviewee P-03 recommended that we add the response category "I don't know," which would allow the researcher to make a better distinction between firms that

did not have certain measures in place versus firms that had the measures in place but did not communicate them effectively.

Interviewee P-03 suggested that the survey should ask if the respondent's firm (or prior firm) had previously been involved in litigation involving electronic discovery, suggesting this would provide the researcher with two additional pieces of information. First, it would provide a potential source for the respondent's awareness of the issues; and second, if the respondent answered affirmatively, it would also provide us with additional information regarding the respondent's perception of the potential risk to the enterprise. Both suggestions will be taken under advisement for future research.

Cyber-Forensic Survey

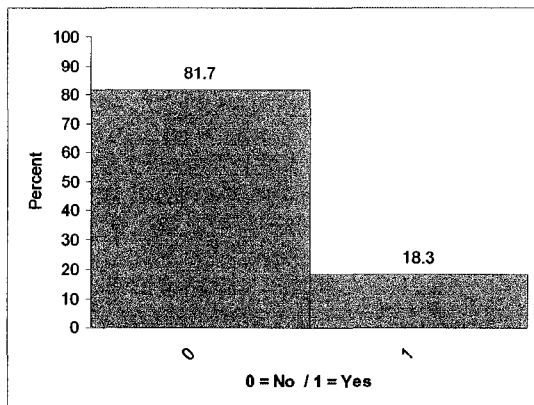
As previously noted, each interview participant was asked and willingly agreed to complete the same survey questionnaire that was previously administered in a pilot study conducted by Dr. Al Marcella, the results of which have been published in the text, *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes [2nd ed.]* (Marcella and Menendez, 2008). The survey questionnaire was used in the course of this research with Dr. Marcella's express permission. As with this follow-up research, Dr. Marcella's study was conducted "in an effort to assess the overall state of cyber forensics awareness and response readiness that existed among firms represented" (Marcella and Menendez, 2008, p. 331). The surveys distributed in Dr. Marcella's pilot study were distributed among "internal and external auditors (financial, operational and IT), security professionals, and IT managers ... and were [t]hus a population that would have more direct exposure and potentially

more direct knowledge of the subject being surveyed ... provid[ing] us a deeper and clearer insight into just how well-prepared and aware the respondents are to the larger picture that is cyber forensics” (pp. 331-332). The research conducted in the course of that pilot study occurred in the same timeframe that the amendments to the Federal Rules of Civil Procedure were enacted into legislation.

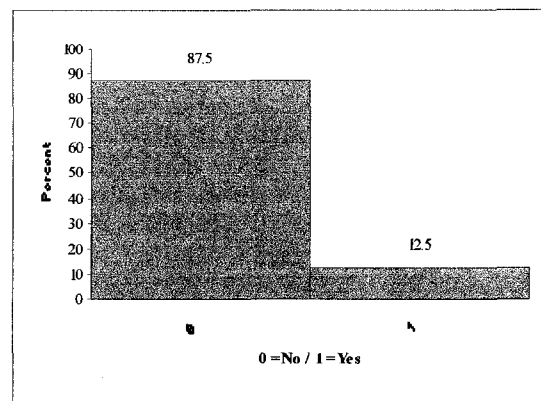
The interview participants for *this* research project came from more varied backgrounds, and the timeframe for the research was approximately 18 months after the amendments were accepted and enacted into law. And while the primary focus of this research was qualitative in nature and the population was much smaller, when examined question-by-question, the results of the two surveys were surprisingly similar and will be examined here individually.¹

Q 01: Does your firm have a cyber forensics response team in place?

Pilot Study



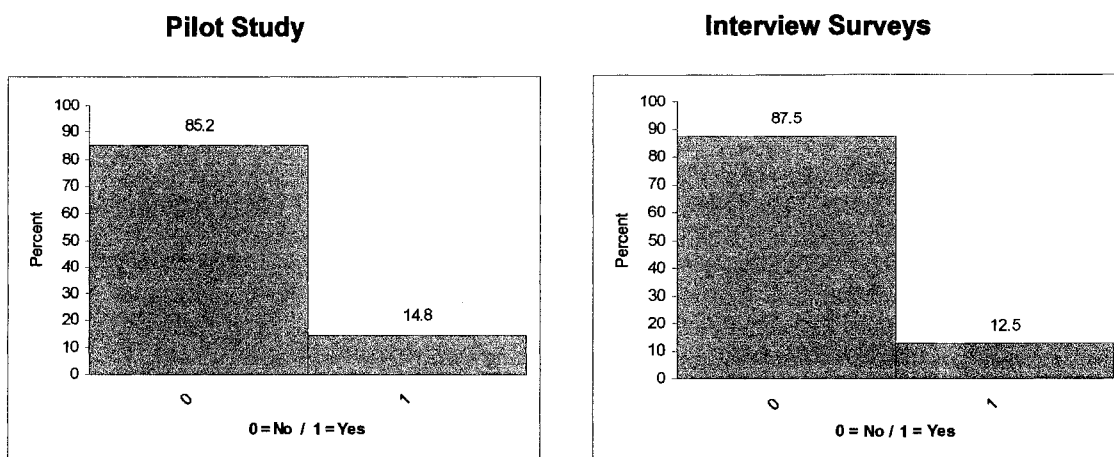
Interview Surveys



¹ Representations from the pilot study are represented here with the author's permission. It should be noted, however, that the representations of the original pilot study were modified slightly, so that the results could be compared on the same scale.

As Marcella notes, “The first question is a very basic one with surprising results. More than 80 percent of respondents noted that their firms either did not have a cyber forensics response team in place, or if they did, the respondent was unaware of its existence” (Marcella and Menendez, 2008, p. 333). As can be seen here, results of the interview surveys were quite similar. Given that the interview participants in this study were from backgrounds that typically would have less exposure and less direct knowledge of the subject matter at hand, it is not surprising that the negative responses are slightly higher.

Q 02: Has your staff received formal training in cyber forensic investigations?

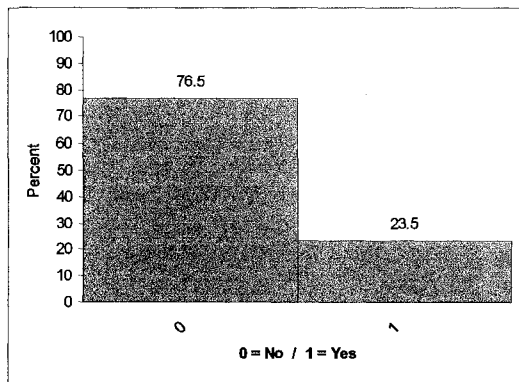


As Marcella further notes, “Given that most of the respondents noted their firms had no formal response teams in place the response to this ... question was not surprising” (Marcella and Menendez, 2008, p. 333), as is also the case with the similarity of responses between the two surveys. More than 85 percent of respondents noted that staff within their organizations had received no formal training in cyber forensic investigations. Not only do the majority of firms represented in these two surveys not have specifically designated individuals

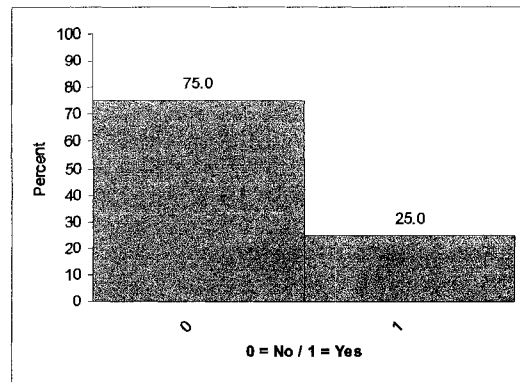
responsible for responding to cyber forensic issues, neither have they provided any formal training regarding proper cyber forensic investigation procedures. This supports the premises of both lack of preparedness and lack of awareness of potential impact on risk to the enterprise.

Q 03: Within the past 12 months, have you met with your legal counsel to discuss internal methods and procedures your staff should follow for engagements that may lead to litigation ?

Pilot Study



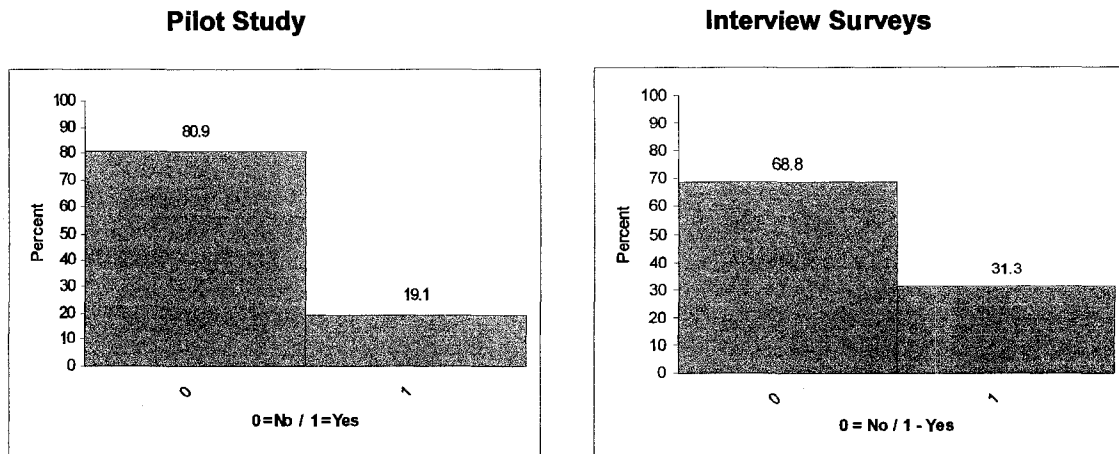
Interview Surveys



In spite of the growing number and types of litigation cases involving electronic discovery, only an approximate 25 percent of respondents in each study stated they had met with legal counsel in this regard. This is only a slight increase over the results of the pilot study, even though the amendments have been in place for more than 18 months since the original pilot study was conducted. “If you consider the growing cost of preparing for e-discovery in litigation cases today, not to mention the size of potential awards [and penalties] that might be involved, these results not only support the premise of lack of preparedness – they suggest

lack of awareness regarding today's litigious climate and significantly increase risk exposure" (Marcella and Menendez, 2008, p. 334).

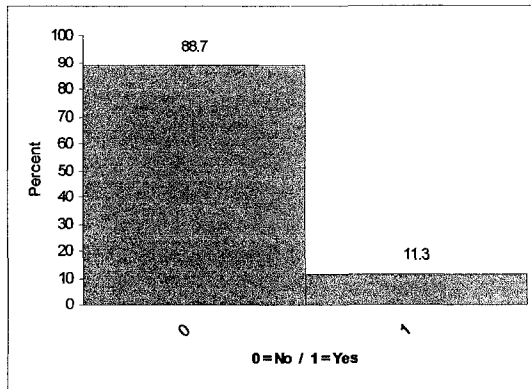
Q 04: Do you have written procedures in place for handling digital evidence ?



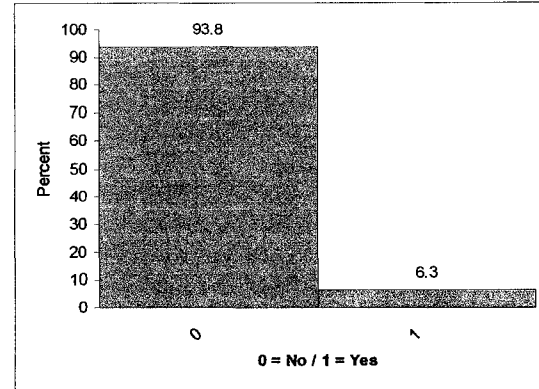
As can be seen in the literature review, and in the results of much of the litigation to date, it is not only important that organizations have written policies in place regarding data retention and data management, it is also of utmost importance that these policies be enforced. And in the event of litigation and / or criminal activities, case outcomes can be won or lost based on proper handling of digital evidence. Yet in the earlier pilot study, more than 80 percent of "those in the know" stated their companies had no written procedures in place for handling digital evidence, with the interview survey following at a close second with nearly 70 percent of respondents noting their organizations had no written policies regarding the handling of digital or forensic evidence. The responses to this question go directly to the heart of the issue of preparedness, and can have a direct impact on risk to the enterprise.

Q 05: Do procedures exist that direct staff on how to conduct a forensic investigation involving digital media?

Pilot Study

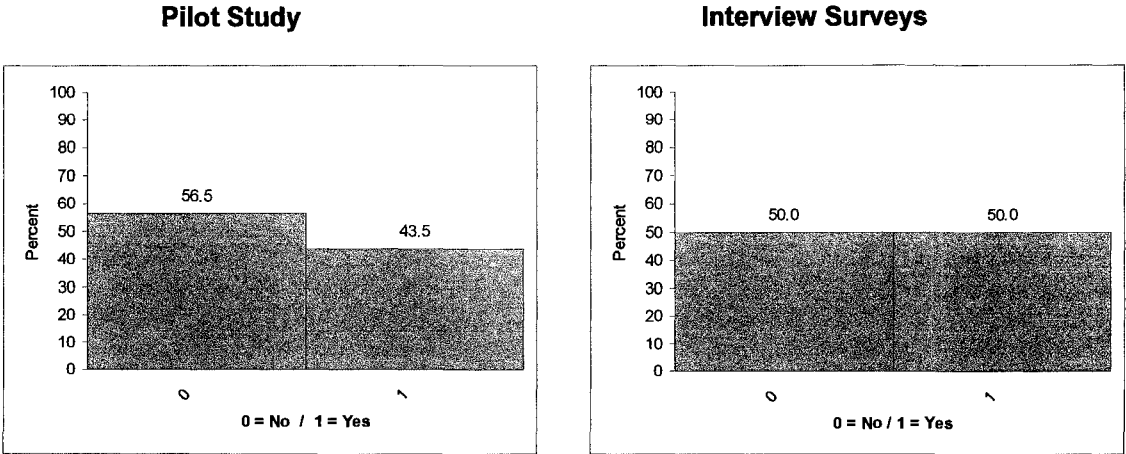


Interview Surveys

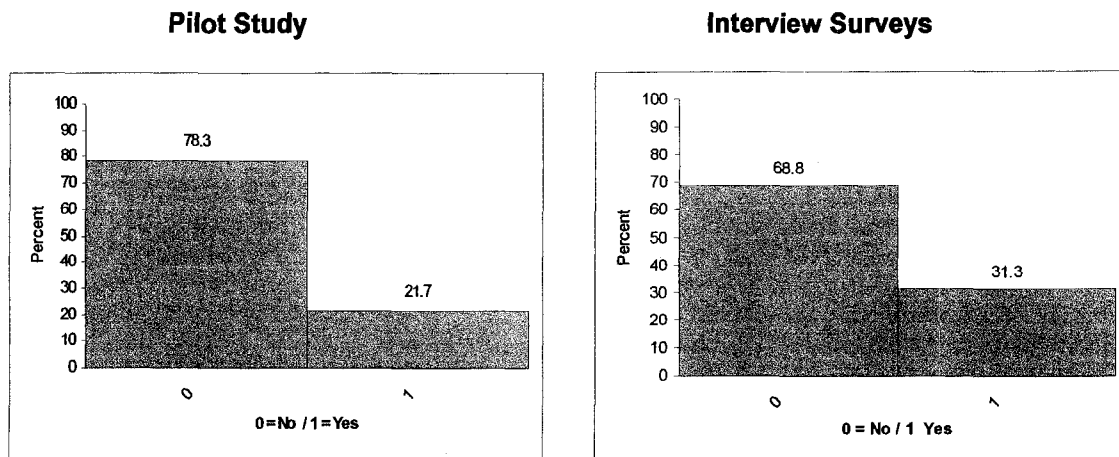


“As landmark cases have shown us, doing the wrong thing can be even more costly than doing nothing at all (e.g., *Perleman vs. Morgan Stanley*: [settlement] \$604.3 million; punitive damages \$850 million)” (Marcella and Menendez, 2008, p. 335). Yet in the case of the pilot study, nearly 90 percent of respondents noted their firms had no procedures in place directing staff on how to conduct a forensic investigation involving digital data; in the case of the interview survey, the results were even higher, approaching 95 percent. This again goes to the issue of lack of preparedness with an increase in potential impact on risk to the enterprise.

Q 06: Does your staff know the proper procedure to follow if field audit work results in the disclosure of inappropriate material on an employee's computer?



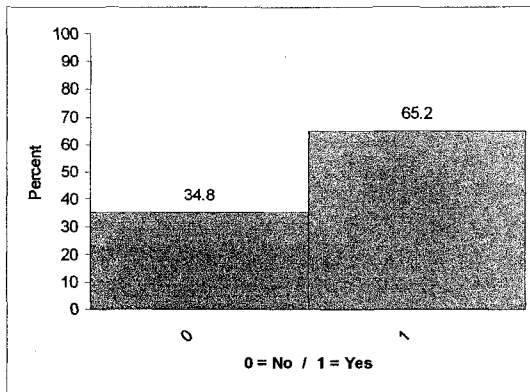
As noted by the interview respondents in human resource roles, a good portion of the litigation a firm faces is in the form of personnel issues and / or wrongful termination cases. And “if the organization becomes involved in issues such as wrongful termination, harassment, or discrimination, the case can easily turn on whether or not the firm followed proper procedures. Even more importantly, when there is internal staff involved, they are far more likely to be aware of your policies (or lack thereof), than an outside litigant” (Marcella and Menendez, 2008, p. 336). Yet the results of both the pilot study and the interview surveys show us that 50 percent or more of the respondents and the firms represented in these two studies do not seem to be aware of what procedures should be followed in the event inappropriate materials are found on an employee's computer. Termination under such circumstances, and resulting litigation of such termination, could have serious impact on enterprise risk.

Q 07: Are these procedures written and distributed to all field auditors?

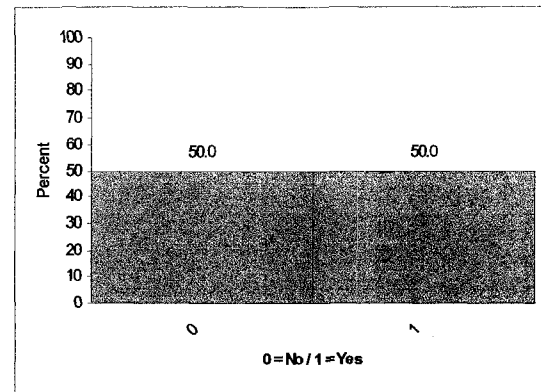
As noted in much of the literature review, if policies and procedures do not exist in written form, they are subject to interpretation, and thus pose more risk to the enterprise; and if these policies and procedures are not disseminated among staff, there is a far greater chance they will not be followed – and enforcement becomes nearly impossible. As previously noted, in the case of the pilot study the respondents were expected to be more knowledgeable in terms of data security and audit policies – yet nearly 80 percent of these respondents noted there either were no written procedures and / or they were not distributed to all field auditors. Similarly, nearly 70 percent of interview survey respondents noted either a lack of written procedures and / or distribution of same. As noted by Marcella and Menendez, “What good are procedures if they are not distributed ... to an organization’s ‘first responders:’ that is, the organization’s audit professionals” (2008, p. 336). Responses to this question address the issues of both lack of awareness and / or lack of preparedness.

Q 08: Does your organization have a policy regarding the disclosure of sensitive internal information, which may become public as a result of a legal deposition?

Pilot Study



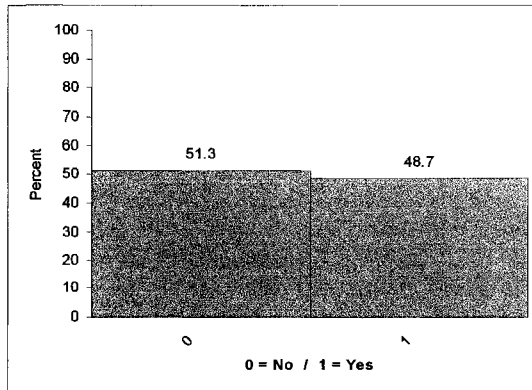
Interview Surveys



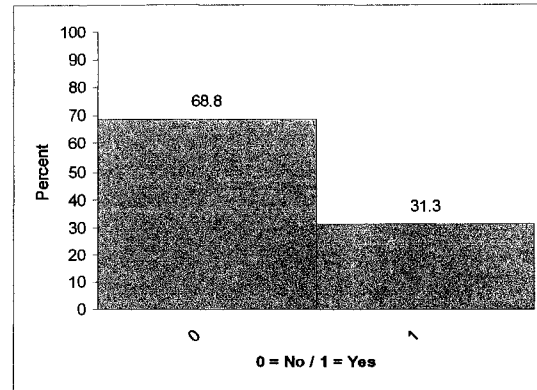
This question could be interpreted to include electronic data as well as any other kind of data (i.e., hard copy data, verbal information, et cetera). Regardless of the type of data involved, this question takes us back to the issue of risk exposure to the enterprise. Whether the data becomes fodder for litigation or not, the organization is still exposed to additional risk if sensitive information is disclosed, particularly if that information is subject to any of the multitude of regulations regarding privacy. If the data does become embroiled in litigation, the exposure to risk is heightened and may well affect both the outcome and the size of the potential settlement involved; and in fact, the inadvertent disclosure of sensitive information may well prove to be the catalyst that leads to the litigation in the first place.

Q 09: Do policies and procedures exist which address exactly what data your organization will (or can) release, when such data is requested by a plaintiff's attorney?

Pilot Study



Interview Surveys

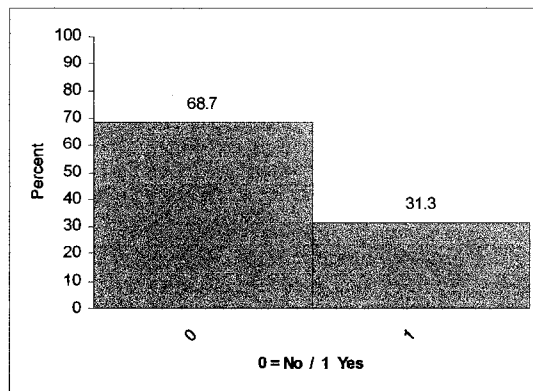


Not only does this question involve information that may be internally sensitive or potentially damaging to the firm, it may also involve privileged information or work products involving the organization's clients. In the latter case, this could result in further liability to the organization and its reputation. When engaging in various forms of client representation or consultancy, there is an implied duty to preserve both the rights and the privacy of those clients. Should a client's rights be violated, and should this breach of trust result in losses to the client (real or imagined), not only can the organization be held liable for such losses, the resultant publicity and damage to the firm's reputation may not be recoverable. Based on the results of the two surveys, we note that more than 50 percent of the organizations represented in the original pilot survey, and nearly 70 percent of the organizations represented in the interview surveys, do not appear to have policies and procedures addressing what data can or will be released upon request. Furthermore, it is probably safe to assume that there are also no policies and procedures in place regarding verification that the requestor is indeed the

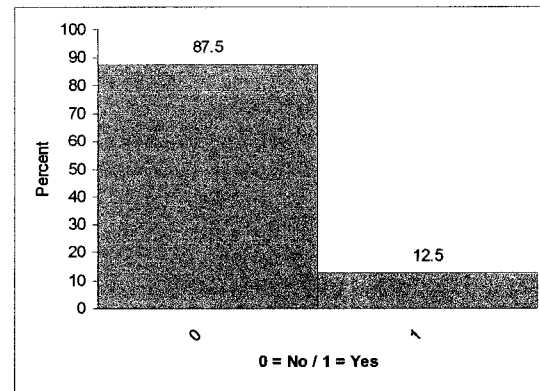
plaintiff's attorney and legally entitled to that data, or any other data being requested.

Q 10: Are procedures in place to prevent non-relevant data, data unrelated to a cyber forensic investigation, from being released or disclosed as part of a larger examination of an employee's suspect activities?

Pilot Study



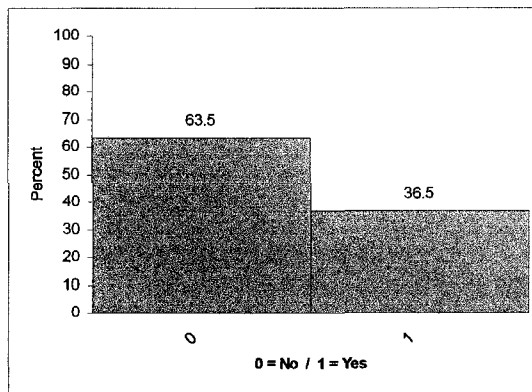
Interview Surveys



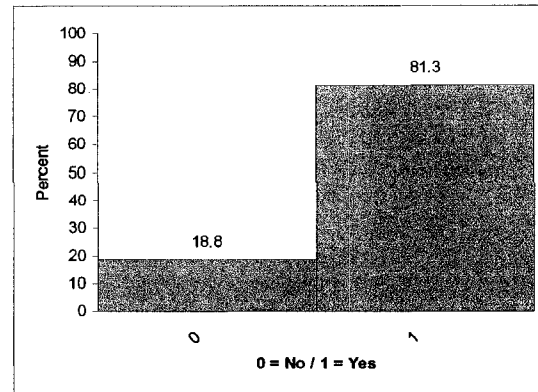
Taking this same issue a step further, nearly 70 percent of respondents from the original pilot survey have no procedure in place to prevent the release or disclosure of non-relevant data in the course of a broader examination of suspect employee activities. “This may be an even larger issue if the non-relevant data is sensitive or considered intellectual property or whose disclosure may violate corporate, government or even customer privacy policies. By not having specific procedures in place that allow for the separation of unrelated, non-relevant data, the organization risks the potential of having to turn over all of its data, due to an inability to separate out just the data requested by a plaintiff's attorney” and only that which is relevant to the case at hand (Marcella and Menendez, 2008, p. 337). Once again, responses to this question are relevant to both the level of preparedness of the firm and potential risk exposure to the enterprise.

Q 11: Are policies in place within your organization that address preservation of data integrity and the archiving of a terminated employee's workstation (e.g., hard drive), in the event that those data may need to be examined after the fact?

Pilot Study



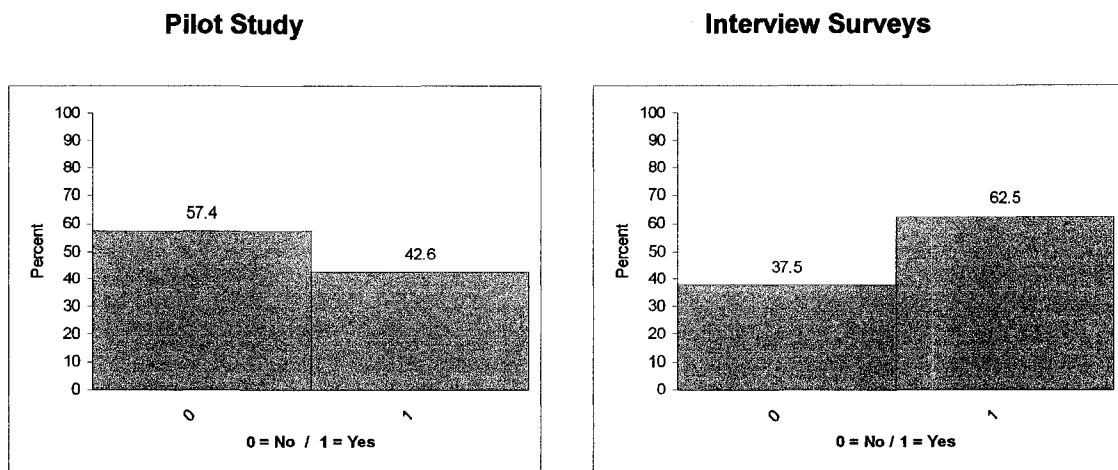
Interview Surveys



Upon termination of an employee, whether voluntary or involuntary, it is typically standard practice within most organizations to immediately disable access rights to all internal information / systems, as well as restricting access to the physical premises (i.e., changing door codes, retrieving electronic entry / access cards, et cetera). And as previously noted by interview respondents who have responsibility for human resources, a large number of litigation issues involve matters of termination, or the cause of such termination. "That being said, it is even more important that [an] organization ensure any and all pertinent data is preserved and data integrity remains intact. Should related issues go to litigation, it will be very important that the firm be able to show that established policy was followed" (Marcella and Menendez, 2008, p. 338). In the original pilot study, 63.5 percent of respondents noted that their firms did not have policies in place that address preservation of data integrity and the archiving of the employees' workstation. Responses from the interview surveys, however, showed significantly

different results, with only 18.8 percent stating their firms did not have such policies in place. This is the first major difference of note between the two studies, which would tend to indicate that the level of awareness has increased and organizations are becoming better prepared in this area. Based on some of the comments made in the course of the interviews, it would appear that this improvement is largely the result of prior litigation involving terminations.

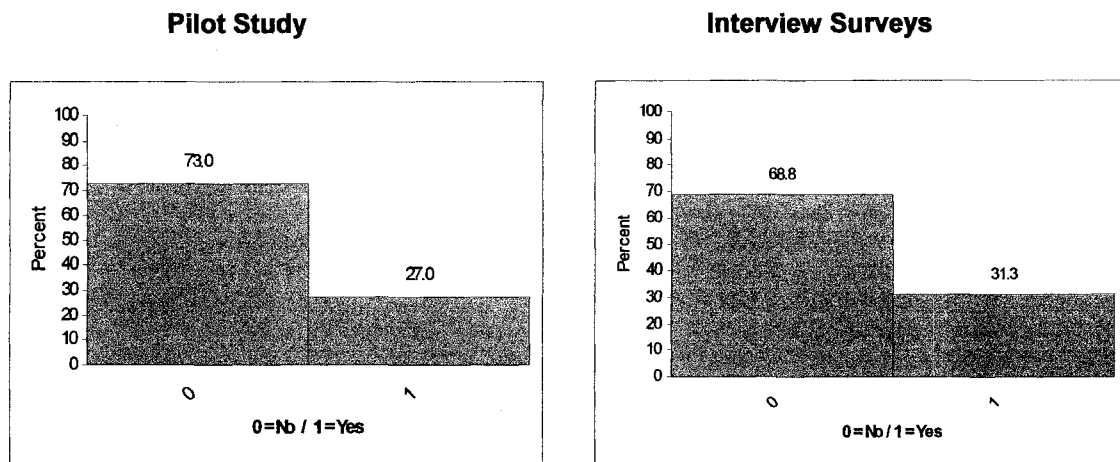
Q 12: Is there a retention policy for such preserved and archived data?



Whether we are dealing with litigation involving termination or any other type of litigation, it is not only important that data integrity be maintained and the data be preserved, it is also important that all applicable regulatory guidelines be adhered to. Regulations pertaining to retention requirements vary by type of data, as well as by industry, and are also affected by the organization's policies and procedures (preferably *written* policies and procedures) regarding data management and data retention. Here, we see an improvement in the level of perceived preparedness between the two surveys, as negative responses

decreased from 57.4 percent to 37.5 percent. Again, based on remarks made in the course of the interviews, this may be the result of experience with prior litigation involving terminations.

Q 13: Would you be able to demonstrate that controls are in place that would prevent any unauthorized access to these archived data that could result in the manipulation or destruction of these archived data?



Based on the responses to the previous questions on the survey, without the appropriate policies and procedures in place, it does not come as a surprise that on average, approximately 70 percent of respondents acknowledged that the firms represented in these two studies would not be able to demonstrate that proper controls were in place which would ensure data preservation and data integrity by preventing unauthorized access to archived data. While we see a slight improvement in the interview surveys (4.2 percent), it is clear that the level of risk exposure to the organization is still an issue in this area.

Statistical Analysis of Survey Results

Descriptive statistics for both the original pilot study and the interview surveys can be found in Tables 5 and 6, respectively, which follow.

Table 5

Descriptive Statistics – Original Pilot study

Descriptive Statistics - Original Pilot Study								
	Count	Mean	Variance	Standard Deviation	P-value	Chi- Square (df=5)	% "NO"	% "YES"
Q 01	115	0.18	0.15	0.39	2.23E-112	530.36	0.817	0.183
Q 02	115	0.15	0.13	0.36	1.24E-121	573.21	0.852	0.148
Q 03	115	0.23	0.18	0.43	2.64E-100	474.43	0.765	0.235
Q 04	115	0.19	0.16	0.40	3.25E-110	520.34	0.809	0.191
Q 05	115	0.11	0.10	0.32	7.47E-132	620.51	0.887	0.113
Q 06	115	0.43	0.25	0.50	4.31E-74	352.83	0.565	0.435
Q 07	115	0.22	0.17	0.41	4.35E-104	491.96	0.783	0.217
Q 08	115	0.65	0.23	0.48	1.39E-81	387.61	0.348	0.652
Q 09	115	0.49	0.25	0.50	1.79E-72	345.31	0.513	0.487
Q 10	115	0.31	0.22	0.47	2.92E-86	409.31	0.687	0.313
Q 11	115	0.37	0.23	0.48	1.32E-79	378.43	0.635	0.365
Q 12	115	0.43	0.25	0.50	1.43E-74	355.05	0.574	0.426
Q 13	115	0.27	0.20	0.45	1.84E-93	442.70	0.730	0.270
Minimum for sample		0						
Maximum for sample		1						
Range for sample		1						
Error for sample		14.38						
Confidence interval		95%						

Table 6

Descriptive Statistics – Interview Surveys

Descriptive Statistics - Interview Surveys								
	Count	Mean	Variance	Standard Deviation	P-value	Chi- Square (df=2)	% "NO"	% "YES"
Q 01	16	0.13	0.12	0.34	7.99E-11	46.50	0.875	0.125
Q 02	16	0.13	0.12	0.34	7.99E-11	46.50	0.875	0.125
Q 03	16	0.25	0.20	0.45	4.14E-08	34.00	0.750	0.250
Q 04	16	0.31	0.23	0.48	3.69E-07	29.63	0.688	0.312
Q 05	16	0.06	0.06	0.25	1.38E-12	54.63	0.938	0.063
Q 06	16	0.5	0.27	0.52	6.14E-06	24.00	0.500	0.500
Q 07	16	0.31	0.23	0.48	3.69E-07	29.63	0.688	0.312
Q 08	16	0.5	0.27	0.52	6.14E-06	24.00	0.500	0.500
Q 09	16	0.31	0.23	0.48	3.69E-07	29.63	0.688	0.312
Q 10	16	0.13	0.12	0.34	7.99E-11	46.50	0.875	0.125
Q 11	16	0.81	0.16	0.40	2.49E-09	39.63	0.188	0.813
Q 12	16	0.63	0.25	0.50	1.76E-06	26.50	0.375	0.625
Q 13	16	0.31	0.23	0.48	3.69E-07	29.63	0.688	0.312
Minimum for sample		0						
Maximum for sample		1						
Range for sample		1						
Error for sample		3.20						
Confidence interval		95%						

Range of the mean scores for the original pilot study varied from a low of 0.11 to a high of 0.65 (0.54); and the range for the interview survey varied from a low of 0.13 to a high of 0.81 (0.68). Variance for the original pilot study ranged from 0.10 to 0.25; and variance for the interview surveys ranged from 0.06 to 0.27 – overall ranges of variance of 0.15 and 0.21, respectively. Likewise, the range of standard deviations for both sets of surveys was also similar, with a range of 0.32 to 0.50 (0.18) for the original pilot study; and a range of 0.25 to 0.52 (0.27) for the interview surveys. As can also be seen for each set of surveys, the resultant *p-values* for each question approximated 0.00, and each had a significant *chi-square*

value. Similarities in the statistics and the ranges would tend to indicate a correlation between the results of the two surveys.

These similarities led the researcher to postulate the hypothesis

$$H_0: \text{Group 1 results} = \text{Group 2 results}$$

where Group 1 represents the results of the original pilot study, and Group 2 represents the results of the interview surveys. Table 7, below, shows the results of the *t*-test for pooled variance between the two groups. As noted in Lind, Marchal, and Wathen, “[I]f the *p*-value is very large, then it is likely that H_0 is true. If the *p*-value is small, then it is likely that H_0 is not true” (2008, p. 343). Thus, with a *p*-value of 0.7321 (two-tailed), we fail to reject the null hypothesis.

Table 7

Hypothesis Test: Independent Groups (*t*-test, pooled variance)

Hypothesis Test: Independent Groups (<i>t</i> -test, pooled variance)		
Group 1	Group 2	
0.68962	0.66369	mean
0.15589	0.22027	std. dev.
13	13	n
24 df		
0.025923 difference (Group 1 - Group 2)		
0.036410 pooled variance		
0.190815 pooled std. dev.		
0.074844 standard error of difference		
0 hypothesized difference		
0.35 t		
.7321 p-value (two-tailed)		

Results of Hypothesis Test: Paired Observations for the two sets of surveys can be found in Tables 8-a and 8-b, which follow.

Table 8-a

**Hypothesis Test: Paired Observations
Pilot Study vs. Interview Surveys ***

Hypothesis Test: Paired Observations

0.000000 hypothesized value
0.689615 mean Group 1
0.663692 mean Group 2
0.025923 mean difference (Group 1 - Group 2)
0.172269 std. dev.
0.047779 std. error
13 n
12 df

0.54 t
.5974 p-value (two-tailed)

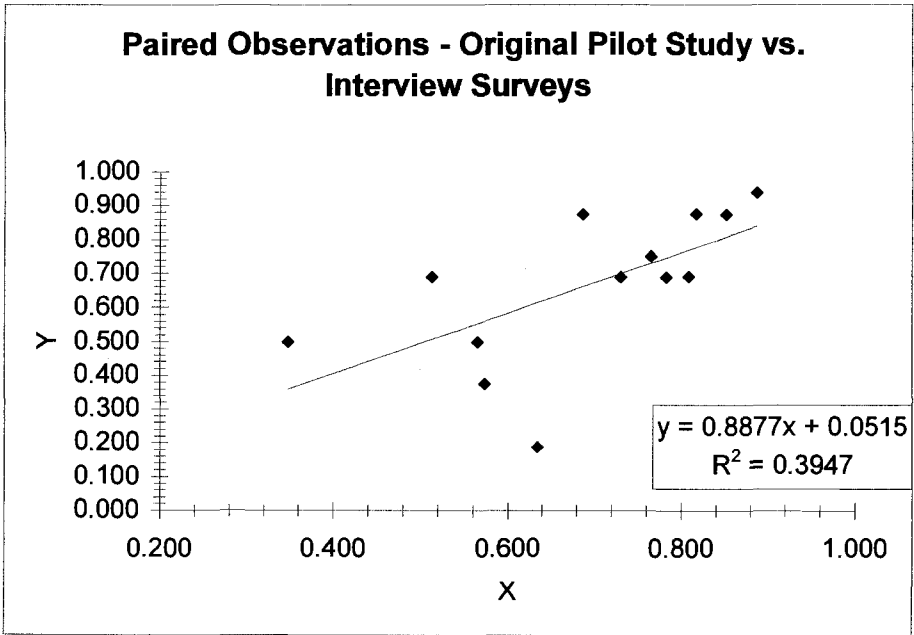


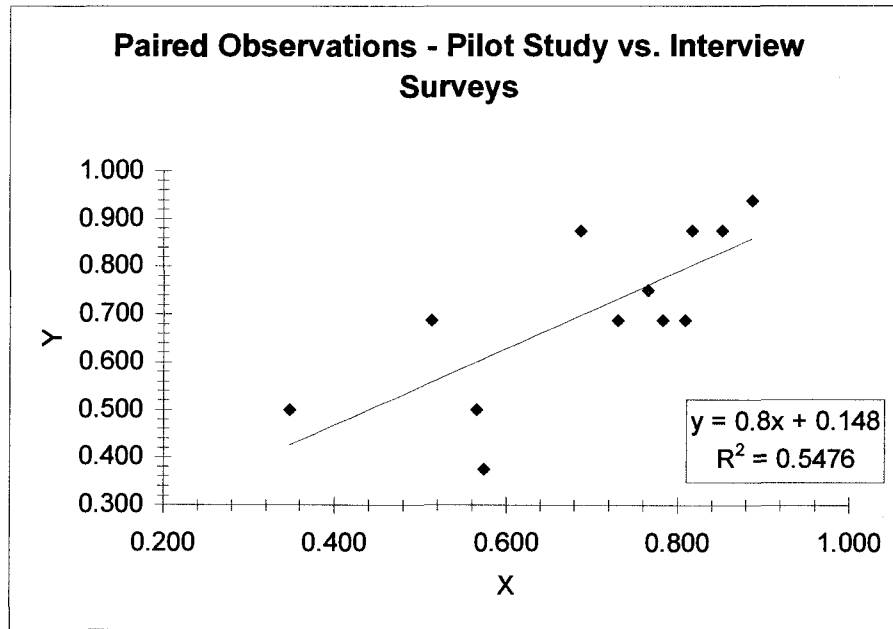
Table 8-b

**Hypothesis Test: Paired Observations
Pilot Study vs. Interview Surveys ***

Hypothesis Test: Paired Observations

0.000000 hypothesized value
 0.694167 mean Group 1
 0.703333 mean Group 2
 -0.009167 mean difference (Group 1 - Group 2)
 0.122118 std. dev.
 0.035252 std. error
 12 n
 11 df

 -0.26 t
 .7996 p-value (two-tailed)



* Outlier (Survey Question Q11) removed.

Table 8-a above, with the results of all questions included, shows us a coefficient of correlation of $R^2 = 0.394$ and a *p-value* of 0.5974 (two tailed). As can be seen in the scatterplot, the correlation is there, if not a tight fit. As noted in the descriptions of the results of each individual question on the survey, the only significantly different result occurred in survey question

Q 11: Are policies in place within your organization that address preservation of data integrity and the archiving of a terminated employee's workstation (e.g., hard drive), in the event that those data may need to be examined after the fact?

Table 8-b above, shows the Hypothesis Test: Paired Observations for the two sets of surveys, with this one piece of outlier data removed. The resultant coefficient of correlation has increased to $R^2 = 0.5476$ (a 15% increase) and *p-value* of 0.7996 (two tailed), indicating a somewhat stronger correlation between the results of the two studies, with the exception of this one data point.

The final analysis conducted was a Goodness of Fit Test, wherein the observed values from the Interview Surveys were compared to the expected values as found in the Pilot Study. As can be seen in Table 9, which follows, this test resulted in a chi-square value of 0.61, and a *p-value* of 1.0000 (df=12). With a *chi-square* value this small and a *p-value* of 1.0000, this would indicate that the observed values of the Interview Survey do not differ substantially from those of the original Pilot Study.

Table 9
Goodness of Fit Test
Pilot Study vs. Interview Surveys

Goodness of Fit Test				
Interview Survey	Pilot Test			
observed	expected	O - E	O - E) ² / E	of chisq
0.875	0.817	0.058	0.004	0.68
0.875	0.852	0.023	0.001	0.10
0.750	0.765	-0.015	0.000	0.05
0.688	0.809	-0.121	0.018	2.97
0.938	0.887	0.051	0.003	0.48
0.500	0.565	-0.065	0.007	1.23
0.688	0.783	-0.095	0.012	1.89
0.500	0.348	0.152	0.066	10.91
0.688	0.513	0.175	0.060	9.81
0.875	0.687	0.188	0.051	8.45
0.188	0.635	-0.447	0.315	51.70
0.375	0.574	-0.199	0.069	11.33
0.688	0.730	-0.042	0.002	0.40
8.628	8.965	-0.337	0.609	100.00
.61 chi-square				
12 df				
1.0000 p-value				

Summary of Statistical Analysis

As noted above, several statistical analysis were conducted to compare the results of the original pilot study to the results of the surveys completed in the course of the interview surveys. In comparing the survey results on a question-by-question basis, the results to all but one question were notably similar. Even though the sample size of the original pilot study was more than seven times that of the interview surveys, the ranges of variance and standard deviation of the samples were similar. The resultant *p-values* and *chi-square* values supported the

hypothesis that the results of the studies would be similar on a question-by-question basis.

Additional statistical analyses were also conducted to compare the overall results of the original pilot study to the results of the surveys completed in the course of the interview surveys, including:

- Hypothesis Test: Independent Groups (*t-test*, pooled variance);
- Hypothesis Test: Paired Observations (with and without outlier value);
and
- Goodness of Fit Test.

All supported the premise that the overall results of each group of surveys would be similar – i.e., that we fail to reject the hypothesis

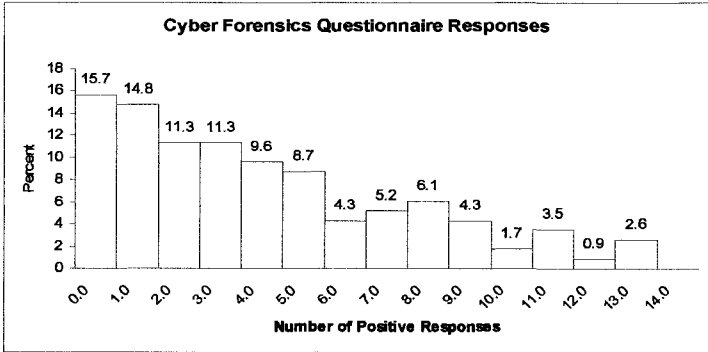
H_0 : Group 1 results = Group 2 results.

Summary of Findings

The objective of this research study was to investigate the level of awareness of organizations regarding the amendments to the Federal Rules of Civil Procedure (FRCP) that were enacted into legislation on December 1, 2006, the ultimate effects of that awareness on the organizations' policy actions, and the resultant level of organizational preparedness in the event of litigation involving electronic discovery. The methodology employed was based on face-to-face interviews, and included the completion of a cyber-forensic survey used in an earlier pilot test. A triangulation of the data obtained in the course of the interviews, the data from the original Pilot Study, and the data from the Interview Surveys all serve to support the following conclusions:

1. More than 18 months after the enactment of the amendments to the FRCP, there is still a relatively low level of awareness of these amendments.
2. Each source of data also serves to support the conclusion that there has been little, if any, effect on organizational policy-making based on the potential impact of the new amendments.
3. While there has been a perceived improvement in the level of preparedness of these organizations regarding potential litigation involving electronic discovery, this improvement has been more the result of experience factors (i.e., current or previous litigation) and other regulatory requirements such as the Sarbanes-Oxley Act (SOX), requirements of the Equal Employment Opportunity Commission (EEOC), the Gramm-Leach-Bliley Act (GLBA), et cetera.

As can be seen below, in the original Pilot Study, Marcella noted that, “only 24 percent of the [original] respondents were able to answer ‘yes’ to more than half of the questions posted [in the survey]; and if we were to consider an academic score of 70 percent to represent a passing grade of preparedness, less than 13 percent of respondents would have made the mark” (Marcella and Menendez, 2008, p. 333).



While the authors go on to note the limited generalizability of the results of the Pilot Study due to the limited sample size, the results of the original Pilot Study, as well as the results of this research project, “clearly indicate that more work – and more research in this area [are] warranted” (Marcella and Menendez, 2008, p. 341).

Chapter V

CONCLUSIONS

Research Goals

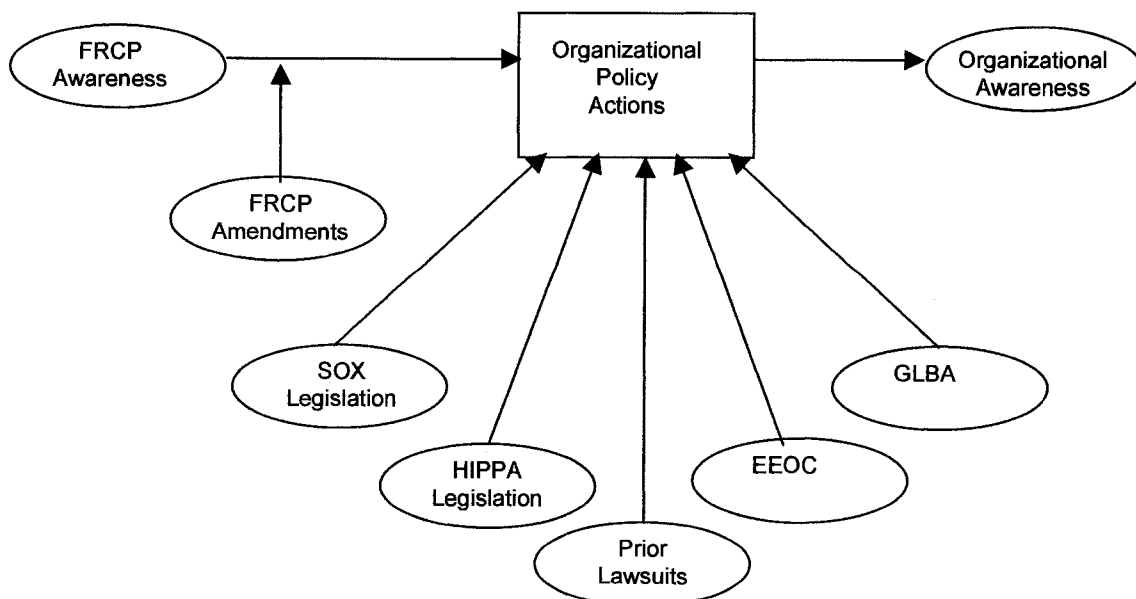
This research reviewed the relationships between the level of awareness of organizations regarding the Federal Rules of Civil Procedure (FRCP), the amendments thereto that were enacted into law on December 1, 2006, the ultimate effects of that awareness on the organizations' policy actions, and the resultant levels of organizational preparedness in the event of future litigation involving electronic discovery. The information gathered will provide relevant and useful information to assist in the assessment of cyber-forensic awareness and preparedness of organizations in an effort to mitigate the potential negative impact of E-discovery on enterprise risk. Focus for this research was based on assessing the level of awareness of the FRCP, and the relationship of that awareness to organizational policy actions, which ultimately result in cyber-forensic preparedness, or lack thereof. Another goal of the research was to compare results of a cyber-forensic survey to the results of a pilot study, which was conducted over the course of several months.

Interview Findings

Interviews were conducted with individuals considered to be in mid- to senior-level management positions representing various functional areas of their organizations. These individuals were selected to determine the range of cyber-forensic awareness in the typical organization, through all areas of the business, and in particular, the range of awareness relating to the Federal Rules of Civil Procedure (FRCP) as they relate to E-discovery. As much of the literature

suggests, a major lack of awareness of the FRCP and the recently enacted amendments appears to be prevalent.

As qualitative research seeks “to learn more from participants through exploration,” (Cresswell, 2005, p. 45), and to “explicate the ways people in particular settings come to understand, account for, take action, and otherwise manage their day-to-day situations” (Miles and Huberman, 1994, p. 7), it provides the researcher with the flexibility to develop a theory, inductively, as new information illuminates the issues and relationships under study. In this study, the researcher began with the hypothesis that awareness of the Federal Rules of Civil Procedure and the recently enacted amendments to those Rules would have a causative effect on the organization’s policy activities, which would in turn impact the organization’s level of cyber-forensic preparedness. While this still appears to be the case to some degree, results of the interviews revealed that there are other moderating factors to be considered – notably awareness of other data-related legislation and previous involvement with litigation involving electronic discovery. The resultant framework is depicted as follows:



This new framework proved an interesting point. While the Federal Rules of Civil Procedure and the amendments thereto have the potential of a more far-reaching impact on risk to the enterprise, to date they appear to have had little or no effect on organizational policy actions as they relate to organizational preparedness to comply with the eventuality of electronic discovery in the event of litigation. Additionally, there is a far greater awareness of other legislation relating to data retention requirements, most notably the Sarbanes-Oxley Act.

To summarize the results of the interviews in terms of the primary and subordinate research questions, there was a low level of awareness regarding both the Federal Rules of Civil Procedure, as well as the amendments thereto, and there was a low level of awareness regarding the impact those amendments might have on enterprise risk for the organizations represented. It is important to keep in mind, however, that these results were based on the perceptions of only one individual in each of the firms represented, and may not be representative of the organizations as entire entities. It is also important to keep in mind that the population of interviewees was not a large sample (only 16 individuals), and was confined to businesses in the St. Louis area. Individuals with different roles in these same organizations, or individuals with the same roles in other branches / locations of these same organizations may have responded very differently.

In terms of the primary and subordinate research questions this study sought to answer, the results of the interviews tend to indicate:

- *Primary Research Question:* the level of awareness of the newly enacted amendments to the Federal Rules of Civil Procedure (FRCP) within and

among the various functional areas of the businesses / individuals represented in this study is almost non-existent.

- *Subordinate Research Question (1)*: the level of awareness of the potential impact of the new amendments to the FRCP on enterprise risk among the businesses / individuals represented in this study is almost non-existent.
- *Subordinate Research Question (2)*: while there was little to no awareness of the FRCP or the amendments thereto, the majority of individuals represented in this study felt their organizations were prepared to comply with those Rules and amendments in the event of litigation involving electronic discovery.

While wide-scale generalizations based on these results would not be warranted, the results would propose the following hypotheses for further study:

- H₁ : Level of awareness of the newly enacted amendments to the Federal Rules of Civil Procedure = 0;
- H₂: Level of awareness of the impact of the new amendments on enterprise risk = 0; and
- H₃: Level of preparedness of the organization to comply with the new amendments > 0.

Survey Results

While the number of surveys completed in the course of these interviews is not large enough to draw generalized conclusions, as can be seen in Appendix G, the results of the surveys are well-aligned with the results of the same surveys as completed in the pilot study. This is further supported by the results of the various statistical analyses that were performed, which compared the two sets of surveys;

and by the interview responses to those questions pertaining to the level of awareness of the amendments to the Federal Rules of Civil Procedure, and to the level of awareness of the potential impact of the amendments on enterprise risk. Yet, while the interview responses seem to indicate a higher level of preparedness to effectively comply with the requirements of electronic discovery, the results of both sets of surveys would seem to contradict this perception.

Areas for Future Study

Neither the original Pilot Study nor this Interview Study involved sample sizes large enough to yield generalizable results. However, “the analysis ... while broad in its potential application, certainly speaks volumes to the fact that as a discipline, the application of cyber forensics and the implementation of cyber forensic investigation techniques are in their infancy and organizational awareness to establishing and implementing policies and procedures dealing with the various elements of cyber forensics, almost non-existent” (Marcella, 2007). Cyber forensics in general, and cyber forensic techniques in particular, offer a wide range of potential opportunities for future research.

Another area that has yet to come into its own is the area of Enterprise Risk Management (ERM). “As companies around the world struggle to comply with the Sarbanes-Oxley Act of 2002, or one of the growing list of regulations modeled after the law, [including the amendments to the Federal Rules of Civil Procedure], they want to make sure that the resources they’re expending benefit the business” (Roth, 2007, p. 55). Yet none of today’s literature on ERM notes any links to the risks imposed by litigation involving electronic discovery – risks that can be mitigated with appropriate planning. With the rising growth rate in litigation across

the globe, today – not to mention the rising costs of discovery – why do we not see any reference to these types of risk in the literature regarding ERM? “After all, Sarbanes-Oxley deals with financial reporting risks and controls; ERM deals with *all* risks and controls” (p. 55). Furthermore, “enterprise risk management (ERM) [is] a way to leverage [an organization’s] investment in compliance and convert it into a shareholder value strategy like cost containment or revenue enhancement. ... Only when risk management is woven into the fabric of the business in this fashion will everyone in the organization understand the importance of risk and incorporate it into their everyday decision making” (Adams and Campbell, 2005, p. 16).

Another area of growing importance involves the retention and management of e-mail. With the growing volume of data, and particularly e-mail data, has come a wealth of new data management systems – and suffice it to say, not all data management systems are created equal. There is a growing need for assessment of the various products available in terms of what data they manage, how that data is managed, and the levels of effectiveness that are provided in terms of both data classification schemes and data retrieval operations. Levels of effectiveness should be evaluated in terms of storage / retrieval costs, time to retrieval, and accuracy of classifications for both inbound and outbound e-mail data.

There is a clear indication that many roles will be changing. The changes brought about by the new E-discovery rules will affect “every business, organization and person that may ever be involved in a federal court case” (Curtis, 2006, p. 1), or any other case involving electronic discovery. And sooner or later, that will involve nearly every business organization, in one way or another. CIOs,

risk managers, and legal counsel will need to work together in ways they never have before this. As Michael Gold, senior partner with Jeffer Mangels Butler & Marmaro, noted, “ ‘It’s a corporate cultural change, and it will take a fair amount of time to work out’ ” (Sloat, 2006).

In their text, *From Business Strategy to IT Action*, Benson, Bugnitz, and Walton noted the growing importance of IT’s involvement in the strategic planning process and the frequent disconnects in this area. Perpetuating the silos that exist between business and IT will no longer be an option. “Culture predefines IT’s role in the business, and limits what and how IT can contribute” (Benson, Bugnitz, and Walton, 2004, p. 214). It has become more important than ever that top management examine that culture and assess these relationships in a new light.

It is important that we all “[k]eep in mind that, in the knowledge economy, everyone is his or her own records custodian” (Spira, 2007, p. 3). Most of us give only our passing attention to those emails that come from IT with regards to policies and procedures that relate to record retention compliance. “The reality is that it is often worse to have a document retention policy that is not followed – or followed in an inconsistent fashion – than no policy at all” (Boehning and Twiste, 2006. p. 58).

Recommendations

Despite the growing complexities involved with electronic discovery and the soaring costs of production, “courts apparently have now reached the point where clients and counsel will no longer be given a pass ... in this day and age a claim of failure to understand the technology sounds like an excuse along the lines of ‘the dog ate my homework.’ Courts today expect inside and outside counsel to be fully

versed in their clients' policies and practices for retaining electronic records and to understand how to preserve and produce relevant electronic records in litigation. The bottom line: Counsel and clients can expect that their conduct in preserving and producing electronic records will more frequently become subject to judicial scrutiny" (Weiner, 2005, ¶ 18). There are a number of steps that can be taken by both the organization and its counsel that can help improve the organization's level of preparedness. "An assessment is the logical first step in identifying how serious the vulnerabilities might be" (Guinaugh, 2003, p. 6). Taking these steps, or failing to take them, can have a profound impact on the final outcome of litigation, whether your organization is the plaintiff or the defendant in the litigation.

The recommendations which follow are hardly all-inclusive, but they will hopefully serve as a place to start. For those firms in a position to do so, it is highly recommended that consultative advice be sought on a proactive basis from professionals with proven experience in designing data management / forensic readiness plans. For those firms facing, or preparing to face litigation involving electronic discovery on a potentially large scale, it is highly recommended that expert forensic expertise be sought as early as possible. "The golden rule is 'do nothing' – at least not without expert advice. Jumping into a fact-finding expedition with electronic data not only is dangerous but also could result in legal sanctions" (Lewis and Gray, 2006, p. 36). Every time a computer is turned on or off, data may be lost or modified, and it is very important to ensure the preservation and integrity of the data involved. It is also important to remember that "collecting the data as early as possible has advantages that are only limited by the settlements awarded in modern litigation" (Lewis and Gray, 2006, p. 37).

Recommendations For the Business

Be intimately familiar with your information systems

“Lawsuits these days require companies to comb through electronic archives and are sometimes won or lost based on how the litigants perform these tasks (EnCase Legal Journal, November 2005)” (Marcella, 2006, p. 3). The best way to ensure that is to begin with understanding all aspects of your information systems: the volume; the architecture; what data is available, and where; what data is accessible, and how. Businesses should “audit their retention policies and computer systems architecture to understand where and how they store ESI, and whether it is readily accessible or not” (Gibson, 2006, p. 7). It is important that you have policies and procedures in place that deal with data retention in the normal course of business.

Designate “Litigation Response Contact(s)”

It is also recommended that companies “consider designating one or more knowledgeable individuals within the information technology group as ‘litigation response contacts’ ” (Ropple and Wolkoff, 2007, p. 3). These individuals should provide counsel with the knowledge they will need about the organization’s information systems. They should keep counsel up-to-date on the “location, accessibility, and retention of ESI.” And in the event of litigation, this individual should “be familiar with the rules, the company’s systems, the ‘inaccessibility’ of ESI, and be well prepared to testify” (Ropple and Wolkoff, 2007, p. 3). Furthermore, “[e]nterprises need to make sure that their outside counsel are technically sophisticated and understand how their computer systems and architecture function” (Gibson, 2006, p. 7). Nelson and Simek further recommend

that, “lawyers... make a quick call to their computer forensics or E-discovery expert and make sure that the expert attends the [pretrial] conference” (2006).

Develop and implement preservation and retention policies

“The process of creating the policy can help the company develop the necessary understanding of its IT systems and compliance with the policy may reduce the volume of material that needs to be searched in responding to discovery requests or a subpoena. The policy should be developed independent[ly] of litigation and should include good faith and reasonable retention requirements for all forms of ESI” (Ropple and Wolkoff, 2007, p. 3). But as David Isom, attorney with Greenberg Traurig LLP in Denver, stated, “document retention needs to be done with litigation accessibility clearly in mind” (Greenwald, 2006). The retention policy should also “provide for the routine disposition of e-data on a schedule that meets business enterprise needs ... a business should dispose of e-data (just like any other documents) on a regular basis in the ordinary course of business, if there is no external reason (e.g., Sarbanes-Oxley or a litigation hold) to retain the e-data” (Gibson, 2006, p. 7).

Document management

Most organizations “simply don’t convert e-mail messages into business records and they vastly underestimate the time, energy and expense required to locate the e-mail records needed in the event of litigation ... By setting policies in place that capture outbound e-mail messages as a business record, an organization can protect itself against unwarranted claims by providing a ‘digital business record’ ” (Rhinehart, 2006). Attorneys at Butler Snow also recommend making sure “the architecture of your system segregates data so preserving

relevant data are possible without disrupting your entire computer operation” (Lofton, 2006, p. 20).

Just as with Dorothy, when she found herself in the Land of Oz, “Traditional records managers often express that same amazement, wonder, befuddlement, and fear when they confront the current state of their discipline. It is a whole new world, a new paradigm, and neither inaction nor minor adaptation is an option. ‘We’re not in Kansas anymore,’ one certified records manager might remark to another” (Arnold, Loos, and Hoke, 2007, p. 55).

Training of Employees

In resolving a problem, it is always good practice to look for the source rather than just treating the symptoms; and in the case of electronic information, particularly e-mail, the source is the employee. “Train your employees on proper workplace e-mail practices to reduce the likelihood of sending inappropriate e-mails. Your employees should be trained about the permanent nature of e-mails, the guidelines for proper workplace e-mails, the need to carefully address e-mails, and how to handle confidential information in electronic communications. Take control of the situation now and decrease your e-mail risk” (Electronic Discovery, 2007, p. 8).

Risk management

“The definition of corporate risk now includes not only financial exposure, but also, the risk of negative public perception of one’s business. The proverbial ‘paper trail’ that often determines the outcome of litigation has expanded exponentially in recent years, due to the proliferation of email, instant messaging, and other digital technologies” (Arnold, Loos, and Hoke, 2007, p. 50). Some of the

risks associated with the possibility of facing litigation involving electronic discovery can be mitigated to some degree, and the key to that mitigation is preparedness.

“As your company assesses the wide range of possible events and business impacts, you should consider the continuum of preparedness – the least to the most that you can do to prepare” (Fitzpatrick, 2007, p. 39). Then you are in a better position to determine the risk your organization is willing, or can afford, to take as weighed against the potential cost associated with mitigation of that risk.

“Risk associated with everyday usage of email is more prevalent than you think” (VanderMeer, 2006, p. 65). In a medium to large sized company, the sheer volume of email can be daunting, and “if your employees send and receive a half million messages a day, this could mean that your email system is placing you and your company at risk about 15,000 times every day!” (p. 65). In his article, *Seven Highly Successful Habits of Enterprise Email Managers: Ensuring that your employees' email usage is not putting your company at risk*, VanderMeer (2006) suggests some best practices for e-mail data management. Excerpts of his *Seven Habits* include the following:

1. *Understand what is in your email and how employees are using it.*
 - Knowing what is in their e-mail is now even more critical as a result of regulatory and legal pressures placed on the significance of email as a business record (p. 65).
 - Assessing the content and context of employee e-mail communications is the first step to understanding its usage and determining the associated risk (p. 66).
 - The first habit to adopt is to implement a recurring, semi-annual audit of e-mail content and usage (p. 67).

2. *Go beyond written policies with education and enforcement.*

- To effectively manage the risks of corporate email, at a minimum businesses need to develop formal policies concerning the creation, handling, and disposition of e-mail (p. 67).
- [These policies] need to be understood by employees and enforced within the messaging infrastructure ... [which can] be accomplished through ongoing education and real-time enforcement (p. 67).
- Education must also include awareness of how and why e-mail is being monitored (p. 68).
- It [should] also include an education of executives and non-IT managers as to the impact legislation, regulations and government oversight have on the messaging technology currently being used – or in most cases, not being used – to enforce these policies (p. 68).
- Incorporate a feedback mechanism to measure the effectiveness of the policy deployment and message activity triggering policy activity (p. 68).
- The second habit to implement is to drive awareness of corporate e-mail policy at every opportunity, as well as to let employees know that it is being enforced proactively.

3. *Don't rely on your employees to manage email usage and retention.*

- Relying on end users to monitor e-mail activity, review messages for compliance, and enforce corporate and regulatory policies is simply not practical. Most end users do not realize that once they send an e-mail, they have almost no control over its future. ... As a result, employees are often not aware or even conscious of the potential impact of each e-mail they send (p. 69).
- When users are responsible for categorization of e-mail, some messages that should be classified as business documents are not, and vice versa (p. 69).
- The third habit to adopt is implementing a sound policy-based e-mail retention solution, which does not depend on end user intervention (p. 69).

4. *Look over your shoulder – e-mail management is more than just blocking spam and viruses at the perimeter.*

- Past effort has been predominantly focused on inbound e-mail, while little or no attention has been given to protecting corporate assets from unintentional and even malicious activity of employees (p. 69).

- Both external and internal threats need to be addressed simultaneously and in conjunction with each other for any solution to work (p. 70).
- The fourth e-mail management habit to adopt is to take a holistic view of your email infrastructure and consider all options for best-of-breed solutions (p. 70).

5. *E-mail management and control is not just an IT problem.*

- Even though IT owns overall responsibility for managing email systems, IT will always rely on human resources, legal, and compliance for defining policy criteria and applicable actions (p. 70).
- Corporate and cultural challenges can impede this departmental or resource cooperation – basic communication and shared accountability (p. 70).
 - Regular open communication is necessary for IT to be able to service its internal customers (p. 70).
 - Legal needs to proactively communicate with IT on a regular basis concerning specific requirements for analysis, retention, and discovery of email (p. 70).
- The fifth habit to adopt for better e-mail management requires involving other departments and key stakeholders in the development and decision of e-mail management solutions (p. 71).

6. *Turn down the volume. Eliminate the amount of e-mail to manage with effective policy-based monitoring and control.*

- Effective e-mail management solutions must support the entire e-mail lifecycle including creation, retention, auditing, management, and retrieval, as well as timely purging of e-mail in conjunction with electronic records management systems (p. 71).
- To effectively reduce the sheer volume of retained e-mail, policy-based classification and categorization are necessary ... for determining how long and for what reasons a message should be retained (p. 72).
- The sixth habit to adopt is to focus on reducing the volume of e-mail through effective analysis. This will pay dividends when dealing with retention and policy enforcement (p. 72).

7. *Archive for retrieval, not storage and backup.*

- The fact that companies even contemplate keeping all e-mail for the next 10 years is proof that e-mail archiving and compliance are not

well understood, and implementing policy-based e-mail management is going through growing pains (p. 72).

- Retaining every e-mail may be a safe bet, but it only hinders the single most important function of your archive – retrieval (p. 73).
- E-mail retrieval, however, is only as effective as the archiving activities which placed the messages in the archive (p. 73).
- The final habit to consider adopting is to remember that archiving is about retrieval, not storage. Implement policy-based archiving to improve your retrieval efficiency and reduce risk associated with litigation and legal discovery (p. 73).

There are any number of litigants who can attest to the fact that, in the last decade, trials have been won and lost because of that one electronic “smoking gun” that was found in someone’s e-mail, on someone’s hard drive, or on the organization’s server. And “if it seems unlikely that someone would find the one ‘smoking gun’ e-mail sitting among thousands in *your* server, you’re wrong again. The new rules are supported by technology that can easily scan millions of e-mails and their attachments, to find any relevant documents” (Electronic Discovery, 2007, p. 8).

“Information management has always recognized that vital records are those without which an organization could not continue. In addition, vital records are now those records that prove compliance with high-fine regulations and defend an organization against spurious litigation” (Arnold, Loos, and Hoke, 2007, p. 52). Due to the volume of data itself, as well as the difficulty in properly managing and categorizing that volume of data, e-mail is arguably the greatest challenge facing litigants and counsel alike, who are involved in electronic discovery battles in this, the “E-Age.”

Recommendations for Counsel

There are also a number of things that counsel can do to help prepare their clients and themselves, which can and will result in better data management and better results in litigation. The first step in this process “is to finally recognize that the FRCP Rules have been changed, and therefore, legal professionals have no choice but to adopt the necessary skills, knowledge, and practices to deal with ESI issues in commercial litigation” (Guinaugh, 2006/December, ¶ 3). With technology changing at such a rapid pace, no two occurrences of litigation or crime involving electronic discovery will be quite the same. Counsel, whether internal or external, need to acquire at least some basic understanding of the concepts surrounding electronic data – its creation, its management, and its retrieval. It is more important than ever before that counsel be able to effectively communicate with the client’s IT staff, as well as with forensics experts. In his article, *E-discovery: It’s getting scary out there*, Weiner suggests “other steps counsel can take to operate more effectively in this new world of e-discovery. These include:

1. Pay early attention to key players in the case and issue a written litigation hold with clear descriptions of the types of electronic data that must be preserved. Provide regular written reminders of the hold.
2. Communicate with the client’s IT department early in the case.
3. Develop at the outset of the case a plan for storing and searching the potentially relevant electronic information in consultation with the client’s internal IT managers, internal counsel, and potentially, an outside electronic data expert. ... The plan should also educate the client on its e-discovery obligations and the likely costs of complying with those obligations in the case at hand.
4. Address the scope of electronic discovery with opposing counsel early in the case.

5. Review the electronic records to identify gaps or potential problems ... before making production so unfounded suspicions about the failure to preserve and produce electronic records do not arise when your adversary reviews the production.
6. Document the electronic record-collection process to enable you to support the propriety and diligence of your handling of electronic records.
7. When discovery disputes arise, direct client resources to enable the presentation of proof ... that makes the complex technical issues raised by the discovery requests comprehensible to the court and articulates with specifics the burdens involved in complying with those requests.
8. Advise clients to adopt policies in advance of litigation that provide rational and defensible guidelines on the treatment of electronic documents.
9. Encourage the lawyers on your staff or at your firm to become familiar with the issues raised by electronic discovery and to develop at least a basic understanding of existing technologies” (2005).

Guinaugh further suggests that, in getting prepared to formulate the argument and plan, “it is advisable to insist upon having input into the development criteria to be used by the responding party to identify all responsive materials,” and if that is not a possibility, “at the very least, insist upon full disclosure of all search criteria to be used by any third-party service provider, and litigation attorneys to understand the depth of the search for pertinent evidence” (2006/June, ¶ 6).

Whatever the case may entail, it is important to discuss the process and the Rules of electronic discovery with your client as early as possible – preferably before litigation is imminent. A good first requirement

will have to be the acknowledgment that e-document and e-mail retention and destruction policies is a legal mandate that requires the full attention of senior management and in-house or corporate counsel. It is also strongly recommended that a third-party information security firm with computer forensics experts assist in the development of the policies, procedures, and auditing functions to ensure successful implementation and protective safeguards (Guinaugh, 2003, p. 6).

“A raft of cases now exist that all bear the same message to attorneys: comply with e-discovery required practices or pay the piper. ... Now that the duties are laid out clearly [under the amendments to the FRCP], you have to ask yourself: What will it cost my client – or my firm – if I don’t abide by them? Are malpractice claims a possibility for those who ignore the new rules? You betcha” (Nelson and Simek, 2006, p. 23).

Summary & Conclusions

“Legal thought it had everything under control. It thought it had done its job. The clear lesson is that if legal and IT aren’t playing as a team, everybody loses” (Schwartz, 2006, p. 30). So noted Ephraim Schwartz regarding *Perleman vs. Morgan Stanley*. In this well noted case, Morgan Stanley thought they were complying when they turned over relevant tapes of emails, as instructed by the court. Unfortunately, after opposing counsel signed off, Morgan Stanley’s IT department “suddenly discovered another 120 tapes with additional backed-up messages in a closet” (p. 30). Then still more tapes were found, even after the judge had been notified. And the cost of this little *OOPS*? “Morgan Stanley was fined \$604.3 million in compensatory damages, and \$850 million in punitive damages” (p. 30). Clearly, “the greatest danger to companies – and the danger that can and has resulted in sanctions – is providing inaccurate or incomplete information” (Boehning and Twiste, 2006, p. 58).

In summary, be proactive – anticipate the obvious, act promptly, and act in good faith. As Judge T. S. Ellis III, of the Eastern District of Virginia, is quick to note, “lawyers who are unreasonable or do not act in good faith with respect to the

new amendments will not like anything he has to say” (Nelson and Simek, 2006, p. 23). It is no longer a question of *whether* your organization will have to face an issue of E-discovery, it is a question of *when* it will happen. The time to act is now, and that begins with an assessment of your organization’s culture and readiness. Make use of sources like Benson et al. (2004) that can help you assess the culture and implement a plan to help you make needed changes. Make use of Organizational Development (OD) specialists to help you plan and manage those changes. Make use of audit and forensic specialists to ensure your organization’s existing information management systems meet your business needs, as well as your compliance needs.

When all is said and done, “Failure to get it right can lead to the loss of the most defensible lawsuit or to costly sanctions. Failure to get it right can compound the cost of litigation. Failure to get it right could result in court-ordered intrusion into the company’s system. Failure to get it right may result in ‘death by E-discovery’ ” (Bermel and Smith, 2007, p. 18).

LIST OF APPENDICES**Appendix A –**

The Sedona Principles for Electronic Document Production 92

Appendix B –

Recap of Federal Rules of Civil Procedure Involving

E-Discovery Amendments 87

Appendix C –

Effects of Amendments on Information Technology 91

Appendix D –

Proposed Research Model 92

Appendix E –

Computer Forensics & E-Discovery Case Law Review 93

Appendix F –

Confidential Cyber Forensics Questionnaire 100

Appendix G –

Comparison of Responses to Data from Pilot Study 102

Appendix H –

Interview Consent Form 102

Appendix I –

Audio / Videotape Consent Form 104

Appendix J –

Interview Agenda 105

Appendix A

The Sedona Principles for Electronic Document Production

The following principles were taken directly from *The Sedona Principles:*

Best Practices Recommendations & Principles for Addressing Electronic

Document Production (July, 2005, pp. 12-13).

1. Electronic data and documents are potentially discoverable under Fed. R. Civ. P. 34 or its state law equivalents. Organizations must properly preserve electronic data and documents that can reasonably be anticipated to be relevant to litigation.
2. When balancing the cost, burden, and need for electronic data and documents, courts and parties should apply the balancing standard embodied in Fed. R. Civ. P. 26(b)(2) and its state law equivalents, which require considering the technological feasibility and realistic costs of preserving, retrieving, producing, and reviewing electronic data, as well as the nature of the litigation and the amount in controversy.
3. Parties should confer early in discovery regarding the preservation and production of electronic data and documents when these matters are at issue in the litigation, and seek to agree on the scope of each party's rights and responsibilities.
4. Discovery requests should make as clear as possible what electronic documents and data are being asked for, while responses and objections to discovery should disclose the scope and limits of what is being produced.
5. The obligation to preserve electronic data and documents requires reasonable and good faith efforts to retain information that may be relevant to pending or threatened litigation. However, it is unreasonable to expect parties to take every conceivable step to preserve all potentially relevant data.
6. Responding parties are best situated to evaluate the procedures, methodologies, and technologies appropriate for preserving and producing their own electronic data and documents.
7. The requesting party has the burden on a motion to compel to show that the responding party's steps to preserve and produce relevant electronic data and documents were inadequate.
8. The primary source of electronic data and documents for production should be active data and information purposely stored in a manner that anticipates future business use and permits efficient searching and retrieval. Resort to disaster recovery backup tapes and other sources of data and documents requires the requesting party to demonstrate need and relevance that outweigh the cost, burden, and disruption of retrieving and processing the data from such sources.

9. Absent a showing of special need and relevance a responding party should not be required to preserve, review or produce deleted, shadowed, fragmented, or residual data or documents.
10. A responding party should follow reasonable procedures to protect privileges and objections to production of electronic data and documents.
11. A responding party may satisfy its good faith obligation to preserve and produce potentially responsive electronic data and documents by using electronic tools and processes, such as data sampling, searching, or the use of selection criteria, to identify data most likely to contain responsive information.
12. Unless it is material to resolving the dispute, there is no obligation to preserve and produce metadata absent agreement of the parties or order of the court.
13. Absent a specific objection, agreement of the parties or order of the court, the reasonable costs of retrieving and reviewing electronic information for production should be borne by the responding party, unless the information sought is not reasonably available to the responding party in the ordinary course of business. If the data or formatting of the information sought is not reasonably available to the responding party in the ordinary course of business, then, absent special circumstances, the costs of retrieving and reviewing such electronic information should be shifted to the requesting party.
14. Sanctions, including spoliation findings, should only be considered by the court if, upon a showing of a clear duty to preserve, the court finds that there was an intentional or reckless failure to preserve and produce relevant electronic data and that there is a reasonable probability that the loss of evidence has materially prejudiced the adverse party.

Appendix B

Recap of Federal Rules of Civil Procedure Involving E-Discovery Amendments

Rule 1

“Rule 1 provides that the Federal Rules be ‘administered to secure the just, speedy, and inexpensive determination of every action’” (The Sedona Conference, July, 2005, p. 2).

Rule 16(b)

“Counsel should also be prepared to discuss electronic discovery issues during the Rule 16(b) pretrial conference with the court, whether required by local rule or not” (The Sedona Conference, July, 2005, p. 19). “[T]he scheduling order entered under this rule may now include provisions for disclosure or discovery of electronically stored information and may now include any agreements the parties reach for asserting claims or privilege or protection as trial-preparation material after production” (Court Rules, 2006).

Rule 26

“Rule 26 requires that any requested discovery be relevant” (The Sedona Conference, July, 2005, p. 2). Under Rule 26(a)(1)(B), the Rule would be amended “to add that a party must, without awaiting a discovery request, provide to other parties a copy of, or description by category and location of, electronically stored information” (Court Rules, 2006).

Rule 26(a)(2)(B)

“The obligation to preserve and produce electronic data may apply to expert witness testimony. The 1993 amendments to Rule 26(a)(2)(B) require the disclosure of all ‘information considered by the [expert] in forming the [expert’s] opinion’” (The Sedona Conference, July, 2005, p. 21).

Rule 26(b)

“Rule 26(b) allows a court to weigh the potential relevance of requested documents against the burden on the party that would have to produce the documents” (The Sedona Conference, July, 2005, p. 2). “Among the factors that must be addressed in electronic discovery are: (a) large volumes of data, (b) data being stored in multiple repositories, (c) complex internal structures of collections of data and the relationships of one document to another, (d) data in different formats and coding schemes that may need to be converted into text to be understood by humans, and (e) frequent changes in information technology” (The Sedona Conference, July, 2005, p. 49).

It should also be noted that “[t]he ordinary and predictable costs of discovery are fairly borne by the producing party. However, Rule 26(b) empowers courts to shift costs where the demand is unduly burdensome because of the nature of the effort involved to comply” (The Sedona Conference, July, 2005, p. 49).

Rule 26(b)(2)(B)

“The amendment to this Rule [provides] that a party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On both a motion to compel

discovery or for a protective order, the burden would be on the responding party to show that the information is not reasonably accessible because of undue burden or cost. Even if that showing is made, the court may nonetheless order discovery from that party if the requesting party shows good cause" (Court Rules, 2006).

Rule 26(b)(2)(i)

"Rule 26(b)(2)(i) provides that discovery may be limited if 'the discovery sought is unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive' " (The Sedona Conference, July, 2005, p. 2).

Rule 26(b)(2)(iii)

"Rule 26(b)(2)(iii) provides for limiting discovery when 'the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues' " (The Sedona Conference, 2005, p. 2).

Rule 26(b)(5)

"When a party withholds information otherwise discoverable under these rules by claiming that it is privileged or subject to protection as trial preparation material, the party shall make the claim expressly and shall describe the nature of the documents, communications, or things not produced or disclosed in a manner that, without revealing information itself privileged or protected, will enable other parties to assess the applicability of the privilege or protection ... The rule does not attempt to define for each case what information must be provided when a party asserts a claim of privilege or work production protection. Details concerning time, persons, general subject matter, etc., may be appropriate if only a few items are withheld, but may be unduly burdensome when voluminous documents are claimed to be privileged or protected, particularly if the items can be described by categories' " (The Sedona Conference, July, 2005, p. 20).

Rule 26(c)

"Allows a court to enter a protective order against burdensome discovery" (The Sedona Conference, July, 2005, p. 2). "These broad powers enable a court to limit discovery of electronic documents or condition their production on cost-shifting if the court concludes that the burden of discovery outweighs its ultimate benefit" (The Sedona Conference, July, 2005, p. 2).

Rule 26(f)

"Requires parties to confer early in litigation to attempt to develop a discovery plan" (The Sedona Conference, July 2005, p. 19). Rule 26(f)(3) & (4) requires that, "when the parties confer pursuant to this rule they discuss any issues relating to preserving discoverable information and any issues related to disclosure or discovery of electronically stored information. This would include the form or forms in which electronically stored information should be produced, and any issues relating to claims of privilege or protection as trial-preparation material. If the parties agree on a procedure to assert such claims after production, the parties should discuss whether to ask the court to include this agreement in an order" (Court Rules, 2006).

Rule 33(d)

“This rule would ... provide that where the answer to an interrogatory may be derived from electronically stored information, and the burden of deriving the answer is substantially the same for the responding party and the requesting party, it is a sufficient answer to the interrogatory to specify the records from which the answer may be derived or ascertained. The responding party would be required to allow the requesting party reasonable opportunity to examine, audit or inspect such records and make copies, compilations, abstracts or summaries” (Court Rules, 2006).

Rule 34

“Permits the service by one party upon another of a request for documents of any type” (The Sedona Conference, 2005, p. 1).

Rule 34(a) & (b)

“The inclusive description of ‘documents is revised to accord with changing technology. It makes clear that Rule 34 applies to electronic [sic] data compilations from which information can be obtained only with the use of detection devices’ ” (The Sedona Conference, July, 2005, p. 2). The rule also provides that “the request may specify the form or forms in which electronically stored information is to be produced. The producing party may object to the requested form or forms for producing electronically stored information stating the reason for the objection. If an objection is made to the form or forms for producing electronically stored information – or no form was made in the request – the responding party would be required to state the form or forms it intends to use. If a request does not specify the form or forms for producing electronically stored information, a responding party must produce the information in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable” (Court Rules, 2006).

Rule 37

“Sets forth guidelines for resolving discovery disputes ... A party that receives a request for production of electronic documents may object to some or all of the request. If such objections are filed and the requesting party opts not to accept the objections, the requesting party must file a motion to compel pursuant to Rule 37” (The Sedona Conference, July, 2005, p. 34).

Rule 37(f)

“Absent exceptional circumstances, a court may not impose sanctions under the 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” (Court Rules, 2006).

Rule 45

“The 1991 amendment to Rule 45 ... requires persons issuing subpoenas to take reasonable steps to avoid imposing undue burdens or expense on the requested party, and, if objection is made, any order to compel production ‘shall protect [the requested party] from significant expense’ ” (The Sedona Conference, July, 2005, p. 51).

Rule 45(c)(1)

“Under a 1991 amendment ... Rule 45(c)(1) requires a party or attorney responsible for the issuance of a subpoena to ‘take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena’ ” (The Sedona Conference, July, 2005, p. 34).

Rule 45(c)(2)(B)

“Provides that, if objection is made to a subpoena, ‘an order to compel production shall protect any person who is not a party or an officer of a party from significant expense resulting from the inspection and copying commanded’ ” (The Sedona Conference, July, 2005, p. 34).

Rule 53(a)(1)(C)

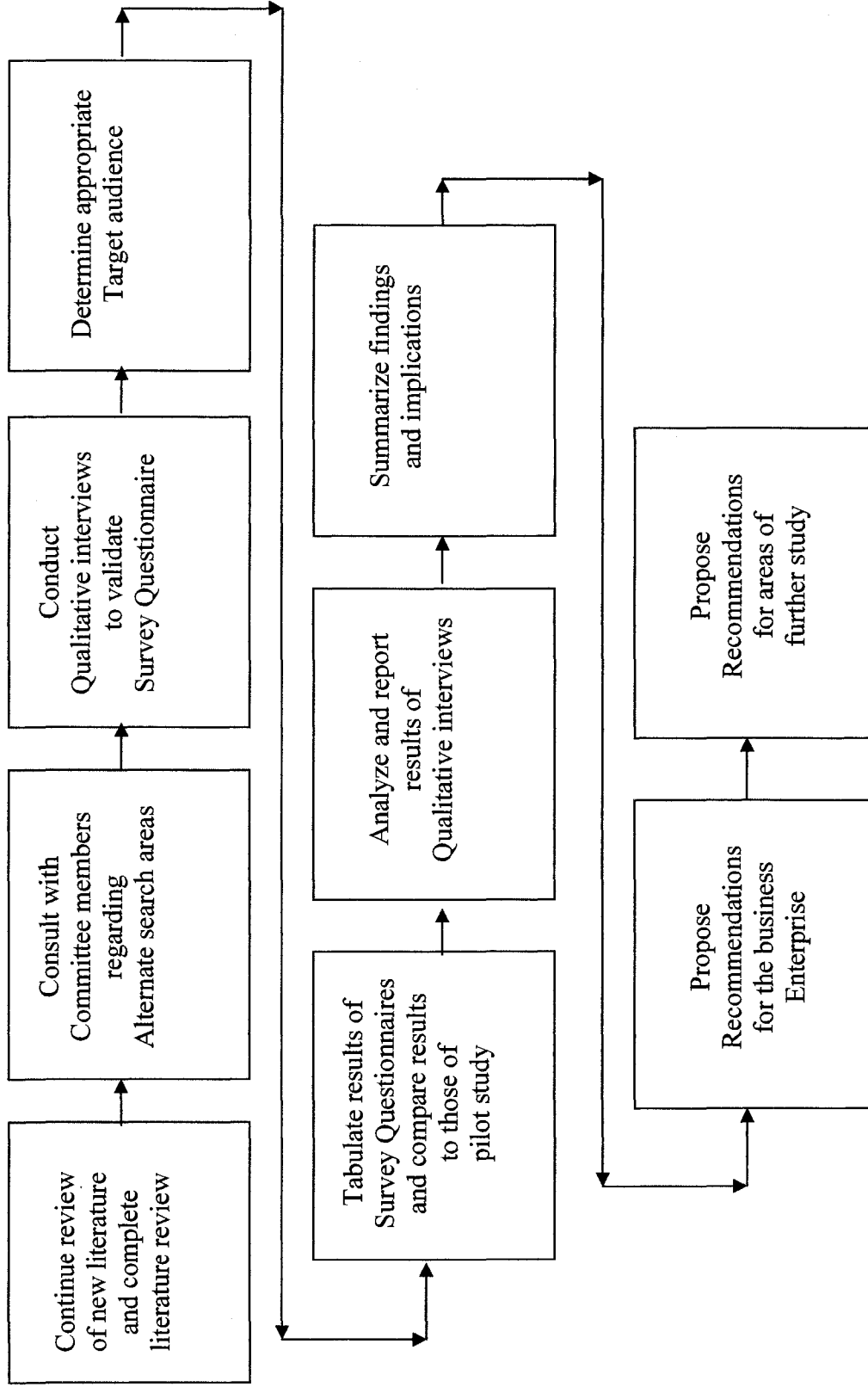
“Use of special masters and court appointed experts to preserve privilege ...One immediate benefit of using such a court appointed ‘neutral’ third part is the probable elimination of privilege waiver concerns with respect to the review of information by that person. In addition, the ‘neutral’ may be able to speed the resolution of disputes by fashioning fair and reasonable discovery plans based upon specialized knowledge of electronic discovery and/or technical issues with access to specific facts of the case [see id]” (The Sedona Conference, July, 2005, p. 40).

Appendix C
Effects of Amendments on Information Technology (IT)

Amendment	Effect on IT
Rule 16(b): A description of all electronically stored information must be presented within 99 days of the beginning of a legal case.	E-mail archiving and retention software and policies should be put in place.
Rule 26(a): Electronically stored information, including e-mail, must be searched without waiting for a discovery request.	IT should put in place e-mail archiving and retention policies so information can be discovered rapidly.
Rule 26(b): A party need not provide discovery of electronically stored information ... if there is an undue burden or cost.	Requires the organization to prove that putting in e-mail archiving software is an onerous expense.
Rule 26(f): Requires litigants to discuss any issues relating to preserving discoverable information.	Requires legal counsel to know how e-mails are being retained and how they can be searched and retrieved.
Rule 34(b): Requires requesting party to designate the form in which it wants electronically stored information to be produced; requires the responding party to identify the form in which records will be produced.	IT must be aware of how e-mails are stored - on disk or tape, for example - and how they will be retrieved.
Rule 37: Establishes a safe harbor provision for deleting records.	Lets IT establish policies for the deletion of e-mail.

(Connor, 2006, p. 16).

Appendix D Proposed Research Model



Appendix E Computer Forensics & E-Discovery Case Law Review

The following is a summary of case law review categories as noted in Federal State Court Rulings on E-Discovery & Computer Forensics as noted on Cyber Controls, LLC website:

Data Preservation & Spoliation

- Danis v. USN Communications
- GTPM v. Wal-Mart
- Keir v. Unum Provident
- Landmark Legal Fund v. EPA
- Linnen v. A.H. Robbins
- Metropolitan Opera v. Local 10 Union
- McGuire v. Acufex crosurgical
- Strasser v. Yalamanchi
- Wiginton v. Richard Ellis

Scope of E-Discovery

- Bethea v. Comcast
- Byers v. Illinois State Police
- Anti-Monopoly v. Hasboro
- McPeak v. Ashcroft
- Fennell v. First Step Design
- Wright v. AmSouth Bankcorp
- Stallings-Daniel v. Northern Trust Company
- Bryant v. Aventis Pharmaceutical
- MHC Investment Co. v. Racom Corp.
- White v. White
- Caldera v. Microsoft Corp.
- Milwaukee Police Assoc. v. Jones
- Playboy Enters Inc. v. Welles
- Itzenson v. Hartford Life and Accident Ins.
- Demelash v. Ross Stores, Inc.
- Collette v. St. Luke's Roosevelt Hospital
- Rowe Entertainment v. The William Morris Agency
- Southern Diagnostic Assoc. v. Bencosme
- In re CI Host, Inc.
- Symantec Corp. v. McAfee Assoc. Inc.
- Storch v. IPCO Safety Products Co.
- Murlas Living Trust v. Mobil Oil Corp

- Crown Life Ins. Co. v Craig
- Lawyers Title Ins. Co. v. U. S. Fidelity & Guaranty Co.
- Santiago v. Miles
- Daewoo Elec. Co. v. United States
- Bills v. Kennecott Corp.

Computer Forensic Protocols

- People v. Carrutu
- United States v. Triumph Capital Group
- State v. Townsend
- United States v. Al-Marri
- Moench v. Red River Basin Board
- Ingenix, Inc. v. Lagalante
- United States v. Bach
- United States v. Tucker
- State v. Guthrie
- Adobe Sys., Inc. v. Sun South Prod., Inc.
- Byrne v. Byrne
- Simon Property Group LP v. mySimon, Inc.
- Playboy Enter. V. Welles
- Easley-McCaleb & Assoc. v. Perry
- First USA Bank v. PayPal, Inc.

Records Management

- Heveafil Sdn. Bhd. V. United States
- Kozlowski v. Sears Roebuck
- Landmark Legal Fund v. EPA
- Public Citizen v. Carlin
- Renda Marine, Inc. v. United States

Forms of Production

- Bristol-Myers Squibb Securities Litig.
- In re Honeywell Int'l, Inc. Securities Litig.
- McNall Tunneling v. City of Evanston

Procedure

- Go 2Net, Inc. v. CI Host, Inc.
- Dodge, Warren, & Peters Ins. Serv. v. Riley
- Gamble v. Deutsche Bank
- Kormendi v. Computer Associates Int'l Inc.
- Advanced Micro Devices Inc. v. Intel Corp.

- Thompson v. Thompson
- The Gorgen Co. v. Brecht
- Tulip Computers Int'l v. Dell Computer
- Murphy Oil USA, Inc. v. Fluor Daniel, Inc.
- Rowe Entertainment, Inc. v. The William Morris Agency
- Columbia Communications v. EchoStar
- Perez v. Volvo Car Corp.
- Benton v. Allstate Ins. Co.
- America Online Inc. v. Anonymous
- Superior Consultant Co. v. Bailey
- United States v. VISA
- Carbon Dioxide Ind. Antitrust Litig.

Production of Data

- Lakewood Engineers v. Lasko Prod.
- York v. Hartford Underwriters Ins. Co.
- Eolas Tech. Inc. v. Microsoft Corp.
- Jones v. Goord
- Kaufman v. Kinkos Inc.
- U. S. Fidelity & Guaranty Co. v. Braspetro Oil
- Braxton v. Farmer's Ins. Group.
- McNally Tunneling v. City of Evanston
- Giardina v. Lockheed Martin Corp.
- Unnamed Physician v. Board of Trustees of St. Agnes Med. Center
- Hayes v. Compass Group USA, Inc.
- McPeck v. Ashcroft
- Kleiner v. Burns
- IL Tool Works, Inc. v. Metro Mark Prod. Ltd.
- Alexander v. FBI
- Smith v. Texaco. Inc.
- Strauss v. Microsoft Corp.
- Easley-McCaleb & Assoc., Inc. v. Perry
- Torrington Co. v. United States
- PHE, Inc. v. Department of Justice
- In re Air Crash Disaster
- Timkenco v. United States
- City of Cleveland v. Cleveland Illuminating Co.
- National Union Elec. Corp. v. Joseph Schlitz Brewing Co.

Privacy & Privilege

- In re Currency Conversion Fee Antitrust Litig.
- Fraser v. Nationwide Mutual Ins. Co.
- United States v. Steward

- United States v. Rigas
- N. Y. State Bar Assoc. Committee on Prof. Ethics
- In re Pacific Gateway Exchange, Inc.
- Minnesota Mining & Mfg. V. Pribyl
- Long Island Diagnostic Imaging v. Stonybrook Diagnostic Assocs.
- Damos v. USN Communications
- Mathias. V. Jacobs

Spoilation

- Liafail, Inc. v. Learning 2000, Inc.
- Antioch v. Scrapbook Borders, Inc.
- Lonbardo v. Broadway Stores, Inc. Rkl Inc. v. Grimes
- Heveafil Sdn. Bhd. v. United States
- Trigon Ins. Co. v. United States
- Penar Software Corp. v. Fortune 500 Sys., Ltd.
- Illinois Toolworks, Inc. v. Metro Mark Prod. Ltd.
- Linnen v. A. H. Robins Co.
- Telecom Int'l Amer., Ltd. V. AT&T Corp.
- United States v. Koch , Ind.
- Lauren Corp. v. Century Geophysical Corp.
- In re Cheyenne Software, Inc. v. Securities Litig.
- National Union Elec. Corp. v. Matsushita Elec. Ind. Co.
- Pearl Brewing Co. v. Joseph Schlitz Brewing Co.
- Adams v. Dan River Mills, Inc.
- Kucala Enters., Ltd. v. Auto Wax Co.
- Stevenson v. Union Pac.
- Procter & Gamble Co. v. Haugen
- Sheppard v. River Valley Fitness One
- Theofel v. Farey Jones
- Tulip Computers Int'l B.V. v. Dell Computer Corp.
- Zubulake v. UBA Warburg LLC

Sanctions

- Hildreth Mfg. V. Semco. Inc.
- Metropolitan Opera Assoc. Inc. v. Local 100
- Residential Funding Corp. v. DeGeorge Fin. Corp.
- Williams v. St. Gobain Corp.
- DeLoach v. Phillip Morris Co.
- Cobell v. Norton
- Sheppard v. River Valley Fitness One
- Procter & Gambel Co. v. Haugen
- Zonaras v. General Motors Corp.
- Toledo Fair Hous Ctr. V. Nationwide Mutual Ins. Co.

- N. Y. State Nat'l Org. for Women v. Cuomo
- Anti-Monopoly, Inc. v. Hasbro, Inc.
- In re Brand Name Prescription Drugs Antitrust Litig.
- Rhône Poulenc Rorer, Inc. v. Home Indemnity Co.
- Williams v. Du Pont
- Delozier v. First Nat'l Bank of Gatlinburg
- Bills v. Kennecott Corp.
- Oppenheimer Fund, Inc. v. Sanders
- Lexis Nexis v. Beer
- Gates Rubber Co. v. Bando Chem. Ind.
- Crown Life Ins. Co. v. Craig
- American Banker Ins. Co. v. Caruth
- Capellupo v. FMC Corp.
- Leeson v. State Farm Mut. Ins. Co.
- National Assoc. of Radiation Survivors v. Turnage
- Invision Media Communications, Inc. v. Federal Ins. Co.
- In re Currency Conversion Fee Antitrust Litig.
- Fraser v. Nationwide Mut. Ins. Co.
- United States v. Rigas
- United States v. Steward
- N. Y. State Bar Association, Committee on Prof Ethics
- In re Pacific Gateway Exchange, Inc.
- Minnesota Mining & Mfg. v. Pribyl
- Long Island Diagnostic Imaging v. Stoneybrook Diagnostic Assocs.
- Danis v. USN Communications
- Mathias v. Jacobs

Forms of Electronic Production

- Adams v. Dan River Mill, Inc.
- Greyhound Computer Corp. v. IBM
- In re Air Crash Disaster
- Minnesota v. Phillip Morris Inc.
- National Union Elec. Corp. v. Matsushita Elec. Co.
- Williams v. Owens-IL, Inc.

Employee Email

- Blakey v. Continental Airlines
- Bourke v. Nissan Motor Corp.
- Smyth v. Pillsbury Co.
- United States v. Bailey

Discovery of E-Evidence Denied

- Fennel v. First Step Design, Ltd.
- Hoffman v. United Telecom, Inc.
- IBM Peripherals EPD Devices Antitrust Litig.
- IBM v. Comdisco, Inc.
- Lawyers Title Ins. v. U.S.F. & G.
- Leeson v. State Farm Ins. Co.
- Muñoz-Santana v. U. S. Immigration Service
- Strausser v. Yalamachi
- U. S. v. Kupka

Admissibility

- J. P. Morgan Chase Bank v. Liberty Mutual Ins.
- Kearley v. Mississippi
- State v. Cook
- Perfect 10, Inc., v. Cybernet Ventures, Inc.
- New York v. Microsoft
- Sea-Land Serv. Inc. v. Lozen Int'l
- Hareston v. State
- V. Cable Inc. v. Budnick
- United States v. Meienberg
- Bowe v. State
- People v. Markowitz
- Hardinson v. Balboa Ins. Co.
- Broderick v. State
- St. Clair v. Johnny Oyster & Shrimp
- SKW Real Estate Ltd. v. Gallicchio
- Monotype Corp. v. Int'l Typeface Corp.
- United States v. Bowers
- United States v. Catabran
- Byers v. Illinois State Police
- In re Bristol-Myers Squibb Securities Litig.
- Rowe Entertainment, Inc. v. The William Morris Agency
- GTFM, Inc. v. Wal-Mart Stores
- Procter & Gamble Co. v. Haugen
- Zonaras v. General Motors Corp.

Costs

- Toledo Fair Hous. Ctr. V. Nationwide Mut. Ins.
- Anti-Monopoly, Inc. v. Hasbro, Inc.
- Rhône Poulenc Rorer, Inc. v. Home Indemnity Co.
- Williams v. Du Pont

- Delozier v. First Nat'l Bank of Gatlinburg
- Bills v. Kellecott Corp.
- Oppenheimer Fund, Inc. v. Sanders
- National Union Elec. Corp. V. Matsushita Elec. Ind. Co.
- Adams v. Dan River Mills
- Pearl Brewing Co. v. Joseph Schlitz Brewing Co.

Appendix F

Confidential Cyber Forensics Questionnaire



CONFIDENTIAL CYBER FORENSICS QUESTIONNAIRE

	Y	N
1. Does your firm have a cyber forensics response team in place?		
2. Has your staff received formal training in cyber forensic investigations?		
3. Within the past 12 months, have you met with your legal counsel to discuss internal methods and procedures your staff should follow for engagements that may lead to litigation?		
4. Do you have written procedures in place for handling digital evidence?		
5. Do procedures exist that direct staff on how to conduct a forensic investigation involving digital media?		
6. Does staff know the proper procedure to follow if field audit work results in the disclosure of inappropriate material on an employee's computer?		
7. Are these procedures written and distributed to all field auditors?		
8. Does your organization have a policy regarding the disclosure of sensitive internal information, which may become public, as a result of a legal deposition?		
9. Do policies and procedures exist, which address exactly what data your organization will (or can) release, when such data is requested by a plaintiff's attorney?		
10. Are procedures in place to prevent non-relevant data, data unrelated to a cyber forensic investigation, from being released or disclosed as part of a larger examination of an employee's suspect activities?		
11. Are policies in place within your organization that address preservation of data integrity and the archiving of a terminated employee's workstation (e.g., hard drive), in the event that those data may need to be examined after the fact?		
12. Is there a retention policy for such preserved and archived data?		
13. Would you be able to demonstrate that controls are in place that would prevent any unauthorized access to these archived data that could result in the manipulation or destruction of these archived data?		

14. What cyber forensics best practices does your firm employ?

15. What is your greatest fear with respect to the emerging importance and impact of cyber forensics to the corporate enterprise?

Thank you for completing the Cyber Forensics Questionnaire. All results will remain strictly confidential and only summary data will be utilized for upcoming research publication.

Appendix G
Comparison* of Responses to Data from Pilot Study
(* comparison of negative responses)

<p>Q 01: Does your firm have a cyber forensics response team in place?</p> <p>86.7% vs. 81.7% from pilot study</p>
<p>Q 02: Has your staff received formal training in cyber forensic investigations?</p> <p>86.7% vs. 85.2% from pilot study</p>
<p>Q 03: Within the past 12 months, have you met with your legal counsel to discuss internal methods and procedures your staff should follow for engagements that may lead to litigation?</p> <p>73.3% vs. 76.5% from pilot study</p>
<p>Q 04: Do you have written procedures in place for handling digital evidence?</p> <p>66.7% vs. 80.9% from pilot study</p>
<p>Q 05: Do procedures exist that direct staff on how to conduct a forensic investigation involving digital media?</p> <p>93.3% vs. 88.7% from pilot study</p>
<p>Q 06: Does staff know the proper procedure to follow if field audit work results in the disclosure of inappropriate material on an employee's computer?</p> <p>46.7% vs. 56.5% from pilot study</p>
<p>Q 07: Are these procedures written and distributed to all field auditors?</p> <p>66.7% vs. 78.3% from pilot study</p>

<p>Q 08: Does your organization have a policy regarding the disclosure of sensitive internal information, which may become public as a result of a legal deposition?</p> <p>46.7% vs. 34.8% from pilot study</p>
<p>Q 09: Do policies and procedures exist, which address exactly what data your organization will (or can) release, when such data is requested by a plaintiff's attorney?</p> <p>66.7% vs. 51.3% from pilot study</p>
<p>Q 10: Are procedures in place to prevent non-relevant data, data unrelated to a cyber forensic investigation, from being released or disclosed as part of a larger examination of an employee's suspect activities?</p> <p>86.7% vs. 68.7% from pilot study</p>
<p>Q 11: Are policies in place within your organization that address preservation of data integrity and the archiving of a terminated employee's workstation (e.g., hard drive), in the event that those data may need to be examined after the fact?</p> <p>13.3% vs. 63.5% from pilot study</p>
<p>Q 12: Is there a retention policy for such preserved and archived data?</p> <p>33.3% vs. 57.4% from pilot study</p>
<p>Q 13: Would you be able to demonstrate that controls are in place that would prevent any unauthorized access to these archived data that could result in the manipulation or destruction of these archived data?</p> <p>66.7% vs. 73.0% from pilot study</p>

Appendix H Interview Consent Form

Consent Form

Electronic Discovery: Awareness of the Recently Enacted Amendments to the Federal Rules of Civil Procedure (FRCP) and Impact on Enterprise Risk

I am conducting research on the level of awareness of the recently enacted amendments to the Federal Rules of Civil Procedure (FRCP) and the impact of those Rules on risk to the enterprise. I am investigating this because I believe awareness of the newly enacted legislation to be the first step in helping organizations better plan to mitigate their risk. This research will consist of an interview that should last between 30 and 60 minutes. Toward the conclusion of the interview, you will be asked to complete a confidential cyber-forensics questionnaire that was used in a recent pilot study in this same field.

If you choose to take part in this project, you will be helping provide valuable information toward future research in this area, and will also gain additional insight and information regarding the newly enacted legislation that may be of benefit to you and your organization, as well. Taking part in this project is entirely voluntary, and no one will hold it against you if you decide not to participate. If you do decide to participate, you may stop at any time without penalty. In addition, you may ask to have your data withdrawn from the study after the research has been conducted.

If you want to know more about this research project, you may contact me by phone, at (314) 724-2085; or by email at SamFitz@swbell.net. This project has been approved by the Institutional Review Board at Webster University.

Information on Webster University policy and procedure for research involving humans can be obtained from Stephanie Schroeder, Ph.D., Chair of the Institutional Review Board, at (314) 961-2660 ext. 7518; or by e-mail at SchroedS@Webster.edu.

You will receive a copy of this consent form.

Sincerely,

Shirley J. Fitzgerald

Doctoral Student

Consent Statement

I agree to take part in this project. I know what I will have to do and that I can stop at any time.

Signature

Date

**Appendix I
Audio/Videotape Consent**

I agree to the audio taping of our interview on _____,
_____, 2008.

Signature

Date

Print Name

I have been advised that I have the right to hear the audio tapes before they are used. I have decided as follows:

_____ I do want to hear the tapes

_____ I do not want to hear the tapes

I do not want to hear the tapes before they are used. I understand that Shirley Fitzgerald and her dissertation committee may use the tapes made of this interview. The original tapes or copies may be used for this research project.
_____ (initials).

Signature

Date

I have had the opportunity to hear the tapes. Shirley Fitzgerald and her dissertation committee may use the tapes made of this interview. The original tapes or copies may be used for this research project. _____ (initials).

Signature

Date

**Appendix J
Interview Agenda**

Name: _____

Title: _____

Organization: _____

Date: _____

**Request to tape record interview.
Assurance of confidentiality.**

1. Introductions, for the record.
2. Are you aware of any of the various laws and regulations regarding data retention?
3. Do you know anything about the Federal Rules of Civil Procedure – what they're about?
4. Do you think these rules might apply to your organization?
5. How might they apply to your role and responsibilities in your organization?
6. Are you aware of the fact that a number of amendments and changes to these Rules went into effect last December?
7. Depending on response to #6: Are you familiar with any of those changes?
8. How do you think those changes might apply to your organization?
9. What kind of impact do you think they might have on your organization?
10. How might they apply to your role and responsibilities in your organization?
11. Do you think these new rules pose any new risk to your organization?
Why/why not?

12. How do you see your role in the organization in relation to those potential risks?
13. In the event of litigation, do you think your organization is prepared to comply with these new rules? Why/why not?
14. Would you be willing to take a short survey dealing with data security and data retention policies within your organization, as you know them?
15. Can you think of any additional questions that might be appropriate or helpful to your organization?
16. Can you think of any additional questions that might be appropriate or helpful to you in your position in the organization?
17. Are there any other questions or comments you would care to add that you think might be helpful to my future research in this area?
18. Do you have any questions for me, anything I can answer or clarify regarding anything we've talked about today?

Closing remarks and thanks.

/saf

References

- Adams, G. W. and Campbell, M. (2005, September). ERM: Walking the Walk on Holistic Risk. *Risk Management Magazine, Volume 52, Issue 9, pp. 16-20*. Retrieved April 16, 2008, from EBSCOHost database.
- Allman, T. Y. (2007, February). E-Discovery in the State Courts: Uniform Rulemaking (or Lack Thereof) and the Ongoing Role of the Sedona Principles. *The Computer & Internet Lawyer, Feb/2007, Volume 24, Number 2, pp. 10-13*. Retrieved February 4, 2007, from EBSCOHost database.
- Allman, T. Y. (2005, January). Proposed National E-Discovery Standards and the Sedona Principles. *Defense Counsel Journal, Jan/2005, Volume 72, Issue 1, pp. 47-55*. Retrieved January 25, 2007, from EBSCOHost database.
- Allman, T. Y. (2003, October). The Case for a Preservation Safe Harbor in Requests for E-Discovery. *Defense Counsel Journal, Oct/2003, Volume 70, Issue 4, pp. 417-423*. Retrieved February 4, 2007, from EBSCOHost database.
- Amendments to the Federal Rules of Civil Procedure. (2006). Retrieved February 11, 2007, from *U.S. Courts: The Federal Judiciary* website at: http://www.uscourts.gov/rules/Ediscovery_w_Notes.pdf
- Arnold, J. R., Loos, H., and Hoke, G. E. (2007, February). We're not in Kansas Anymore: A Risk-Based Approach to Records Management. *AIIM E-DOC, Volume 21, Issue 1, pp. 50-53*. Retrieved April 10, 2007, from EBSCOHost database.
- Barkett, J. M. (2004, October). Bytes, Bits and Bucks: Cost Shifting and Sanctions in E-Discovery. *Defense Counsel Journal, Oct/2004, Volume 70, Issue 4, pp. 334-356*. Retrieved February 4, 2007, from EBSCOHost database.
- Benson, R. J., Bugnitz, T. L., and Walton, W. B. (2004). *From Business Strategy to IT Action: Right Decisions for a Better Bottom Line*. Hoboken, NJ. John Wiley & Sons, Inc.
- Bermel, J., and Smith, A. L. (2007, February). E-Discovery Survival Guide for Corporate Counsel. *St. Louis Lawyer, Volume XLV, Number 10, pp. 13, 18*.
- Boehning, H. C., and Twiste, E. (2006, November). New Rules for Electronic Discovery. *Risk Management Magazine, Nov/2006, Volume 53, Issue 11, p. 58*. Retrieved January 25, 2007, from EBSCOHost database.

- Bosch, W. (2006, November 20). New Discovery Rules Offer Operators Increased Transparency. *Hotel & Motel Management Magazine, Volume 221, Issue 20, p. 11*. Retrieved January 25, 2007, from EBSCOHost database.
- Cohasset Associates. (2006, July). *Making the Case for E-Mail Archiving and Litigation Readiness*. White Paper prepared by Cohasset Associates, Inc.
- Conference of Chief Justices. (2006, August). *Guidelines for State Trial Courts Regarding Discovery of Electronically-Stored Information*. Retrieved January 16, 2008 from <http://www.cybercontrols.net/common/wp.asp>
- Connor, D. (2006, December). New E-Records Rules: Who's Complying? *Network World, December 4, 2006, Volume 23, Issue 47, p. 16*. Retrieved February 4, 2007, from EBSCOHost database.
- Cooper, D. R., and Schindler, P. S. (2003). *Business Research Methods. [8th ed.]*. New York, NY: McGraw Hill Higher Education, A Division of the McGraw-Hill Companies.
- Cortese, A. W., Jr. (2005, October). Proposed Amendments of the Federal Civil Rules Strike a Healthy Balance. *Defense Counsel Journal, Oct/2005, Volume 72, Issue 4, pp. 354-361*. Retrieved January 25, 2007, from EBSCOHost database.
- Court Rules. (2006). *LexisNexis Applied Discovery®: Court Rules*. Retrieved February 11, 2007, from: <https://www.lexisnexis.com/applieddiscovery/lawLibrary/courtRules.asp>
- Creswell, J. W. (2005). *Educational Research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research. [2nd ed.]*. Upper Saddle River, NJ: Merrill Prentice Hall.
- Curtis, C. E. (2006, December). The E-Discovery Awakening. *Securities Industry News, December 4, 2006, Volume 18, Issue 41, pp. 1, 30*. Retrieved February 7, 2007, from EBSCOHost database.
- Cyber Controls, LLC. (2008). Federal and State Court Rulings on E-Discovery & Computer Forensics. Retrieved April 11, 2008, from: www.cybercontrols.net/forensics/attorneyreviews.asp
- E-Discovery Amendments. (2007, January/February). *Secured Lender, Jan/Feb 2007, Volume 63, Issue 1, p. 100*. Retrieved February 4, 2007, from EBSCOHost database.
- E-Discovery Amendments to FRCP Approved. (2006, July/August). *The Information Management Journal, Volume 40, Issue 4, p. 15*. Retrieved February 4, 2007, from EBSCOHost database.

- Edwards, J. (2007, January). Follow the E-Mail Trail. *CFO Magazine, Jan/2007, Volume 23, Issue 1, pp. 25-27*. Retrieved February 4, 2007, from EBSCOHost database.
- Electronic Discovery: The Need for E-Mail Risk Training. (2007, March). *Electrical Wholesaling, Volume 88, Issue 3, p. 8*. Retrieved April 10, 2007, from EBSCOHost database.
- Farrell, G. (2006, December). If There Could be a Case, Then Don't Delete That E-Mail. *USA Today, December 1, 2006*. Retrieved February 4, 2007, from EBSCOHost database.
- Fitzpatrick, G. (2007, February). Risk Intelligent Enterprises: business impact analysis benefits. *Accountancy Ireland, Vol. 39, No. 1*. Retrieved April 13, 2008, from EBSCOHost database.
- Garretson, R. (2006, December). A Lifecycle of Its Own. *CIO Insight, December/2006, Issue 76, pp. 81-89*. Retrieved February 4, 2007, from EBSCOHost database.
- Gassler, F. H. (2002, Spring). Dealing with Discovery in the Too Much Information Age. *FDCC Defense Quarterly, Spring/2002, pp. 513-528*. Retrieved January 25, 2007, from EBSCOHost database.
- Gibson, S. (2006, August). The Urgent Need for E-Data Management at the Enterprise Level: The Impending Implosion of Electronically Stored Information. *The Computer & Internet Lawyer, Aug/2006, Volume 23, Number 8, pp. 5-8*. Retrieved January 25, 2007, from EBSCOHost databases.
- Greenemeier, L. (2006, December). Study Shows IT Security Holds the Key to Compliance. *Information Week, December 4, 2006*. Retrieved February 11, 2007, from:
<http://www.informationweek.com/management/showArticle.jhtml?articleID=196601378&subSection=Compliance>
- Greenwald, J. (2006, December). Electronic Discovery Rules Revised. *Business Insurance, December 18, 2006, Volume 40, Issue 51, pp. 4-6*. Retrieved January 25, 2007, from EBSCOHost database.
- Guinaugh, R. B. (2006, December). Action Speaks Louder than Words. *Cyber Bytes*. Retrieved February 10, 2008, from:
<http://cybercontrols.net/cyberbytes/CyberBytes-12-06.pdf>

- Guinaugh, R. B. (2006, June). When E-Production Simply Doesn't Cut It. *Cyber Bytes*. Retrieved February 10, 2008, from:
<http://cybercontrols.net/cyberbytes/CyberBytes-06-06.pdf>
- Guinaugh, R. B. (2003, September). *Harnessing Digital Evidence*. A CyberControls White Paper. Retrieved February 10, 2008, from
<http://www.cybercontrols.net/common/wp.asp>
- Haig, B. D. (1995). Grounded Theory as Scientific Method. *Philosophy of Education*. Retrieved September 23, 2007, from:
http://www.ed.uiuc.edu/EPS/PES-Yearbook/95_docs/haig.html.
- Lange, M. C. S. (2003, June). E is for Evidence: Using an Online Repository to Review and Produce Electronic Data. *Journal of Internet Law, Jun/2003, Volume 6, Issue 12, pp. 18-21*. Retrieved February 4, 2007, from EBSCOHost database.
- Lewis, P. G. and Gray, B. (2006, October/November). Understanding Data Forensics. *Bank Accounting & Finance, Volume 19, Issue 6, pp. 36-44*. Retrieved February 11, 2007, from EBSCOHost database.
- Lind, D.A., Marchal, W. G., and Wathen, S. A. (2008) *Statistical Techniques in Business & Economics*. [13th ed.]. Boston, MA: McGraw-Hill Irwin.
- Lofton, L. (2007, January). With New Electronic Discovery Rules, Technology Targeted. *Mississippi Business Journal, January 1, 2007, Volume 29, Issue 1, pp. 19-21*. Retrieved January 25, 2007, from EBSCOHost database.
- McMillan, R. (2006, December). Ready to Produce IMs in Court? *CIO Magazine, December 15, 2006, Volume 20, Issue 6, p. 34*. Retrieved January 25 2007, from EBSCOHost database.
- Marcella, A. J., Jr. (2006). Preparing for the Digital Records Storm: ESI, the Law and Corporate Vigilance. Pre-publication copy, received from author on January 8, 2007.
- Marcella, A. J., Jr., and Menendez, D. (2008). *Cyber-Forensics: A Handbook for Field Auditors*. [2nd ed.]. New York, NY: Auerbach Publications.
- Marcus, R. L. (2006). E-Discovery & Beyond: Toward Brave New World or 1984? *Review of Litigation, Symposium 2006, Volume 25, Issue 4, pp. 635-689*. Retrieved January 25, 2007, from EBSCOHost database.
- Marshall, C., and Rossman, G. B. (2005). *Designing Qualitative Research*. [3rd ed.]. Thousand Oaks: Sage Publications.

- Maxwell, J. A. (2005). *Qualitative Research Design: An Interactive Approach*. [2nd ed.]. Thousand Oaks, CA: Sage Publications, Inc.
- Miles, M. B., and Huberman, A. M. (1994). *Qualitative Data Analysis* [2nd ed.]. Thousand Oaks, CA: Sage Publications, Inc.
- Murphy, B. (2005). *The Price of Flawed Electronic Discovery*. Retrieved April 13, 2008, from <http://www.forrester.com/Research/Document/Excerpt/0,7211,37026,00.html>
- Myler, E. (2006, June). The ABCs of Records Retention Schedule Development. *AIIM E-DOC, May/June 2006, Volume 20, Issue 3, pp. 52-56*. Retrieved February 11, 2007, from EBSCOHost database.
- Nelson, S. and Simek, J. (2006, December). The New Federal Rules of Civil Procedure: An ESI Primer. *ABA Law Practice Magazine, Dec/2006, Volume 32, Number 8, p. 23*. Retrieved February 11, 2007, from: <http://www.abanet.org/lpm/magazine/articles/v32/is8/an7.shtml>
- Nelson, S. and Simke, J. (2005, November). Spoliation of Electronic Evidence: This Way be Dragons. *ABA Law Practice Magazine, Nov/2005*. Retrieved February 11, 2007, from: <http://www.abanet.org/lpm/lpt/articles/tch06052.html>
- Preimesberger, C. (2006, November). Saving the Data. *eWeek, November 27, 2006, Volume 23, Issue 47, pp. 11-12*. Retrieved January 25, 2007, from EBSCOHost database.
- Rhinehart, C. (2006, January). E-mail Management for SOX: More than Meets the Eye. *Compliance Pipeline*. Retrieved February 11, 2007, from: <http://www.informationweek.com/177103858>
- Rice, T. E., Sterchi, T. N., and Boschert, T. M. (2005, Winter). Proposed Federal Rules of Civil Procedure Amendments Concerning Electronic Discovery: Will They Be Enough? *FDCC Quarterly, Winter/2005, Volume 55, Issue 2, pp. 155-174*. Retrieved February 4, 2007, from EBSCOHost database.
- Ropple, L. M. and Wolkoff, H. J. (2006). Amended Federal Rules of Civil Procedure Focus on E-Discovery. Retrieved February 11, 2007, from Ropes & Gray LLP website at: <http://www.ropesgray.com>
- Roth, J. (2007, April). Myth vs. Reality: Sarbanes-Oxley and ERM. *Internal Auditor, Volume 64, Issue 2, pp. 55-60*. Retrieved April 13, 2008, from EBSCOHost database.

- Sanders, R. L. (1999, October). Personal Business Records in an Electronic Environment. *The Information Management Journal, Oct/1999, Volume 33, Issue 4, pp. 60-63*. Retrieved January 25, 2007, from EBSCOHost database.
- Scheindlin, S. A., and Wangkeo, K. (2005). *Electronic Discovery Sanctions in the Twenty-First Century*. Retrieved April 13, 2008, from <http://www.mttl.org/voleleven.scheindlin.pdf>.
- Schwartz, E. (2006). Regulation Watch: IT's Day in Court. *InfoWorld, November 20, 2006, Volume 28, Issue 47, pp. 29-33*. Retrieved February 7, 2007, from EBSCOHost database.
- Sedor, D. P. (2006). *The Increasing Risk of Sanctions for Ordinary Negligence in E-Discovery Compliance*. Retrieved April 13, 2008, from Discovery Technology Group™, White Paper Series.
- Shelton, G. D. (2006, October). Don't Let the Terabyte You: New E-Discovery Amendments to the Federal Rules of Civil Procedure. *Defense Counsel Journal, Oct/2006, Volume 73, Issue 4, pp. 324-331*. Retrieved February 4, 2007, from EBSCOHost database.
- Soat, J. (2006). IT Confidential: Supreme Court Says, Show Me the Data. *Information Week, November 13, 2006*. Retrieved February 11, 2007, from: <http://www.informationweek.com/management/showArticle.jhtml?articleID=193700356&subSection=Compliance>
- Solnik, C. (2006, September). E-Discovery Pushes Limits as Law's Digital Dynamo. *Long Island Business News, September 28-October 5, 2006, Volume 53, Issue 41, p. 38*. Retrieved January 25, 2007, from EBSCOHost database.
- Solnik, C. (2006, December). In Law, Electronic Information Becomes the Brave New World. *Long Island Business News, December 22-28, 2006, Volume 53, Issue 60, p. 4B, 14B*. Retrieved January 25, 2007, from EBSCOHost database.
- Spira, J. (2007, January). Electronic Content – a Federal Case. *KMWorld, Jan/2007, pp. 1-3*. Retrieved January 25, 2007, from EBSCOHost database.
- Swann, J. (2007, January). E-mail Becomes Fair Game in Federal Court. *Community Banker, Jan/2007, Volume 16, Issue 1, p. 58*. Retrieved January 25, 2007, from EBSCOHost database.

- The Sedona Conference® Working Group Series. (2005, July). The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production, July 2005 Version. Retrieved February 10, 2007, from http://www.thesedonaconference.org/dltForm?did=7_05TSP.pdf
- The Sedona Conference® Working Group Series. (2005, September). The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age. Retrieved February 10, 2007, from http://www.thesedonaconference.org/dltForm?did=TSG9_05.pdf
- VanderMeer, J. (2006, December). Seven Highly Successful Habits of Enterprise Email Managers: Ensuring that your employees' email usage is not putting your company at risk. *Information Systems Security, Volume 15, Issue 6*, pp. 64-75. Retrieved April 10, 2007, from EBSCOHost database.
- Volonino, L. (2003). Electronic Evidence and Computer Forensics. *Communications of the Association for Information Systems, Volume 12*, pp. 457-468. Retrieved February 11, 2007, from EBSCOHost database.
- Weiner, G. L. (2005, March/April). E-Discovery: It's getting scary out there. *American Bar Association Bulletin, Volume 14, Number 4*. Retrieved May 4, 2008, from <http://www.abanet.org/buslaw/blt/205-3-04/weiner.shtml>.
- Zeidner, R. (2007, January). Employees Don't 'Get' Electronic Storage. *HR Magazine, Jan/2007, Volume 52, Issue 1*, pp. 28. Retrieved February 4, 2007, from EBSCOHost database.