UNIVERSITY OF OREGON
APPLIED INFORMATION MANAGEMENT

Presented to the Interdisciplinary Studies Program:
Applied Information Management and the Graduate School of the University of Oregon
in partial fulfillment of the requirement for the degree of Master of Science

The Impact of the Sarbanes-Oxley Act of 2002 on Computer Forensic Procedures in Public Corporations

CAPSTONE REPORT

Jeremy Mullis
IT Manager
Trailblazer Studios

University of Oregon
Applied Information Management
Program

July 2009

Continuing Education
1277 University of Oregon
Eugene, OR 97403-1277
(800) 824-2714

Approved by

Dr. Linda F. Ettinger

Running Head: IMPACT OF SARBANES-OXLEY

The Impact of Sarbanes-Oxley Act of 2002 on Computer Forensic Procedures in Public Corporations

Jeremy Mullis

Trailblazer Studios

Abstract

The purpose of this literature review is to examine the impact of Sarbanes-Oxley on development of internal security policies and computer forensics strategies. Focus is on selected literature, published between 1999 and 2009, relating to public corporation computer forensics and electronic record retention. Literature reveals that corporations must be able to preserve electronic records, respond quickly to incidents and provide correct information required by law, or risk vulnerability during an audit or investigation.

Table of Contents

Introduction

Problem

Once thought of as strictly a law enforcement responsibility, computer forensics incidents within corporations are now often handled by corporate IT staff and security personnel (Carrier, 2002). According to Nelson, Phillips, Enfinger, and Steuart (2006), computer forensics is defined as "the application of computer investigation and analysis techniques in the interest of determining potential legal evidence" (p. 6). Wikipedia further defines computer forensics as "a branch of forensic science pertaining to legal evidence found in computers and digital storage mediums. Computer forensics is also known as digital forensics" (Computer Forensics, 2009).

Forensic investigations by corporate staff are increasingly commonplace as companies try to handle non-criminal matters internally to avoid negative publicity or lawsuits (Haggerty & Taylor, 2006). In the corporate environment, computer forensics can include multiple types of incidents, including (a) those that are not considered to be within corporate policies, (b) employee abuse, and (c) those that can be defined as criminal activities (Nelson, Phillips, Enfinger, & Steuart, 2006).

Regulatory developments such as the Sarbanes-Oxley Act of 2002 (also known as the Public Company Accounting Reform and Investor Protection Act of 2002) force companies to create plans and policies to prevent and investigate a variety of types of fraud (Richardson, 2005). Sarbanes-Oxley specifically targets publicly traded corporations (not privately held companies)

to prevent and prosecute fraud (Richardson, 2005). According to the description on Wikipedia, "The legislation set new or enhanced standards for all U.S. public company boards, management and public accounting firms. It does not apply to privately held companies. The act contains 11 titles, or sections, ranging from additional corporate board responsibilities to criminal penalties, and requires the Securities and Exchange Commission (SEC) to implement rulings on requirements to comply with the new law." (Sarbanes-Oxley, 2009, para 2).

The assumption underlying this study is that in the event of computer fraud in a company, staff responsible for the investigation should be well versed in the legal, reporting and procedural issues related to Sarbanes-Oxley (Vacca, 2005). In order to maintain compliance with the intent of Sarbanes-Oxley, companies will need to develop internal security policies that not only deter computer-related crime, but also include strategies that align with the guidelines of federal laws (Brown & Nasuti, 2005).

Purpose

According to Brown and Nasuti (2005), managers in publicly held corporations need to feel confident that when an incident is investigated internally, the proper procedures are carried out in order avoid further ramifications if law enforcement or other agencies need to step in. However, a preliminary review of literature pertaining to computer forensics shows a lack of standardization of internal forensic procedures within publicly traded companies due to the large amounts of computer operating systems and legal issues that exist among various business types (Meyers & Rogers, 2004).

The purpose of this literature review is to explore the impact of Sarbanes-Oxley on the development of internal security policies and computer forensics strategies, as these are defined in publicly traded companies. Richardson (2005) posits that Sarbanes-Oxley not only encourages the use of computer forensics, but the laws and regulations inherent in Sarbanes-Oxley cannot be met without the use of computer forensics. The intended outcome is a guide that describes within Sarbanes-Oxley for consideration when developing internal security polices and investigative practices related to collecting and maintaining relevant electronic evidence during internal computer forensic investigations within publicly traded companies.

Audience/ Significance

This paper is directed at security personnel and information managers in publicly traded companies who are in positions that involve development of internal security policies and the practice of computer forensics. IT managers and board members who must understand the forensic impact of Sarbanes-Oxley in order to develop responsible internal governance policies are part of the targeted audience.

The field of computer forensics has expanded beyond the settings of government and law enforcement and is now finding a place in the corporate world (Carrier, 2002). The 2008 Computer Security Institute (CSI) Computer Crime and Security Survey reported that the most expensive security incidents were related to “insider” financial fraud (Richardson, 2008). The reported fraud cases made up 12% percent of the key types of computer forensic incidents and the average loss per reported incident equaled $463,100.00 (Richardson, 2008).

Internal investigations in publicly traded companies are heavily scrutinized in the wake of numerous fraud cases in recent years (Haggerty & Taylor, 2006). These crimes, under the regulation of the federal government, should warrant immediate response in order to comply with Sarbanes-Oxley (Sarbanes-Oxley Act, 2002). Section 409 of Sarbanes-Oxley underscores the importance of speed in investigations and sets punishments for not reporting of incidents in a timely manner (Sarbanes-Oxley Act). In order be in a position to timely report incidents, a company must rapidly respond to internal computer-related activities that can have a profound financial effect on the company (Richardson).

Limitations

Time frame. While computer forensics has been around since the early 1980s, only in the last few years have investigations been instigated by the internal staff of corporations (Carrier, 2002). In order to minimize the risk of including obsolete literature, sources published prior to 1999 are not included. The primary focus is to include relevant literature published in the years following the introduction of Sarbanes-Oxley in 2002.

Sources. Literature is selected from academic journals, books, and government documents. Juried publications are given higher priority over non-juried articles as they are qualified by members of their respective fields and judged to have enough warrant for publication (Leedy & Ormrod, 2005). Because Sarbanes-Oxley primarily targets publicly traded companies within the US, priority is given to US publications.

Topic definition. The decision to focus on impact in relation to Sarbanes-Oxley, rather than other federal compliance laws, is due to the broader nature of the regulation, compared to

others that are centered around healthcare privacy (HIPAA) or specific to only one State, including California SB 1386 (Richardson, 2005).

Focus. This study focuses on the impact that Sarbanes-Oxley has in relation to computer forensics application in publicly held corporations, and in particular on the need to develop record keeping and destruction of electronic records policies in relation to collection and maintenance of relevant evidence. The enforcement of IT policies in corporations that are required to abide by Sarbanes-Oxley creates complications that need review and analysis. Due to the public nature of financial reporting and scrutiny by several regulatory agencies, these publicly held corporations are under heavy pressure to stay in compliance (Brown & Nasuti, 2005)

Audience. The target audience includes IT staff and information security professionals within the corporation who may be placed in a computer forensics role. According to Brown and Natusi (2005), effective IT governance and security are now measured by Sarbanes-Oxley compliance. This means that executives and board members who are ultimately responsible for Sarbanes-Oxley regulated activities are also part of the potential audience for this study (Brown & Natusi, 2005). Because fines and imprisonment for failure to comply with Sarbanes-Oxley are possible, anyone in the organization who is active in corporate security would benefit in this study's content.

According to Wolfe (2007), security policy works when management is active in not only the development the policies but also supporting the policies. In companies that are subject to Sarbanes-Oxley, policies and procedures require special attention to the needs of the company as well as requirements of the law. In cases where computer forensics may come into play, security

policies require careful planning (Müller, 2008). As Sarbanes-Oxley adds layers of complexity to record retention, the amount of potential evidence in corporate data increases and the increase has a direct impact on computer forensics procedures and policies (Volonino, 2003).

Data Analysis Plan Preview

The literature utilized in this review is collected and analyzed using content analysis (Leedy & Ormrod, 2005). Analysis procedures are designed to discover pertinent factors within the Sarbanes-Oxley Act of 2002, related to potential policies and computer forensic strategies for collection and maintenance of relevant evidence within publicly held corporations. To operationalize the approach, an eight step coding process known as conceptual analysis is employed to examine and identify specific key words relating to Sarbanes Oxley and computer forensics in publicly traded companies (Busch et al., 2005), specifically concerning the need to develop record keeping and destruction of electronic records policies in relation to collection and maintenance of relevant evidence.

Writing Plan Preview

This study is designed as a literature review with the intent of examining factors related to the impact of Sarbanes-Oxley on publicly held companies' computer forensics functions in relation to collection and maintenance of relevant evidence. Once the factors are identified through content analysis, they are organized according to a thematic approach as a way to frame the Review of Literature section of this document (UNC, 2007). The use of a thematic approach organizes subject matter around a unifying theme. This study is based on a set of three anticipated areas of concentration, viewed as preliminary themes, including: a) computer

forensics procedures, b) publicly held security policies, and c) the impact of Sarbanes-Oxley in relation to collection and maintenance of relevant evidence.

Definitions

The following definitions are derived from the literature selected for use in this paper. The definitions give the audience an explanation of the major terms discussed in this study to provide clarity. While some of the terms are also defined in other sections of the paper, this section provides an easy way to locate terminology that is unknown or unclear to the audience.

Computer fraud: The intentional deception or misrepresentation of information for financial or other gain using electronic means (Kovacich, 1999).

Computer forensics: According to Nelson, Phillips, Enfinger, and Steuart (2006), computer forensics is defined as "the application of computer investigation and analysis techniques in the interest of determining potential legal evidence" (p. 6). The preservation, identification, extraction, and documentation of computerized evidence using sophisticated tools and procedures (Vacca, 2005). Wikipedia further defines computer forensics as "a branch of forensic science pertaining to legal evidence found in computers and digital storage mediums. Computer forensics is also known as digital forensics" (Computer Forensics, 2009).

Electronic evidence: Electronically stored information on any type of computer device that can be used as evidence. Evidence in digital form can be email, data archives, metadata, network logs, cookies, web usage logs, email, and Instant Messaging logs (Volonino, 2003). Also defined as information stored in a digital format that establishes proof or value in investigations (Nelson, Phillips, Enfinger, & Steuart, 2006).

Computer abuse: Defined by Straub (1990) as "the authorized and deliberate misuse of assets of the local organizational information system by individuals, including violations against hardware, programs, data and computer service (p. 7).

Fraud: Actions that attempt to gain a dishonest advantage including assets misappropriations, corruption and fraudulent statements. Asset misappropriations are the most common form of corporate fraud, making up 85% of total fraud. (Seetharaman, Senthilvelmurugan, & Periyanayagam, 2004).

Information security: The protection of unauthorized access to or modification of information, whether in storage, processing, or transit and against the denial of authorized users or the provision of service to unauthorized user, including those measures necessary to detect, document, and counter such threats (Vacca, 2005, p. 685).

Internal governance policies: "Specifying the decision rights and accountability framework to encourage desirable behaviour in the use of IT. The leadership and organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategies and objectives." (Information technology governance, 2009)

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:Not Bold, Font color: Auto

Publicly traded corporations: Public corporations are companies that are permitted to offer stocks or bonds for sale to the general public through a stock exchange and regulated the Security and Exchange Commission. (Wikipedia, 2009)

Records management: "The practice of maintaining the records of an organization from the time they are created up to their eventual disposal. This may include classifying, storing,

securing, and destruction (or in some cases, archival preservation) of records." (Records management, 2009)

Electronic records policies: A policy consists of the minimum and maximum retention periods for electronic records and the framework for administering the policy (Howell & Cogar, 2003).

Relevant evidence: "Relevant evidence means evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence. All relevant evidence is admissible, except as otherwise provided by the Constitution of the United States, by Act of Congress, by these rules, or by other rules prescribed by the Supreme Court pursuant to statutory authority" (United States, 2006).

Sarbanes-Oxley: The Sarbanes-Oxley Act establishes a set of requirements for financial systems, to deter fraud and increase corporate accountability (National Institute of Standards and Technology (2007). According to the description on Wikipedia, "The legislation set new or enhanced standards for all U.S. public company boards, management and public accounting firms. It does not apply to privately held companies. The act contains 11 titles, or sections, ranging from additional corporate board responsibilities to criminal penalties, and requires the Securities and Exchange Commission (SEC) to implement rulings on requirements to comply with the new law." (Sarbanes-Oxley, 2009, para 2).

Security policy: According to Kissel (2006), **"**A document that delineates the security management structure and clearly assigns security responsibilities and lays the foundation necessary to reliably measure progress and compliance." (p. 56)

Research Parameters

The research parameters section provides information describing the research questions and research design that make up the literature review. The goal of this section is to describe the methods used to create the literature review. Steps taken to search, collect, document and analyze the selected literature are presented, as well as a description of the data analysis and writing plans that the development of the Review of Literature and Conclusion sections of the study.

jmullis 6/4/09 6:27 PM
Deleted: Address question below regarding Main Research Question in the Week 9 document.

jmullis 6/4/09 5:04 PM
Formatted: Bullets and Numbering

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:(Default) Times New Roman

Research Questions and Sub-questions

Main research question. How do the regulations pertaining to record collection and destruction of records in Sarbanes-Oxley alter compliance requirements, defined in computer forensics procedures?

jmullis 6/4/09 5:04 PM
Formatted: Bullets and Numbering

jmullis 6/4/09 6:26 PM
Deleted: What potential impact does Sarbanes-Oxley have on the development of internal governance policies related to the computer forensics practices of publicly held corporations, specifically on the need to develop record keeping and destruction of electronic records policies in relation to collection and maintenance of relevant evidence?
Don't you think this is the main question? Please get back to me regarding your thoughts on this in the Week 9 document.

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:(Default) Times New Roman, Bold, Italic

Sub-questions.

- What does computer forensics mean?
- How has the jurisdiction of computer forensics practice evolved? (Carrier, 2002)
- What is Sarbanes-Oxley?
- What aspects of Sarbanes-Oxley directly impact the application of computer forensics in corporations?
- What is a 'computer forensic incident'?
- What is internal governance?
- To what do 'record keeping' and 'electronic records policies' refer?
- Who is ultimately responsible for complying with Sarbanes-Oxley within IT activities?
- How do governance laws, in particular Sarbanes-Oxley**,** change the way corporations respond to electronic crimes?

Search Strategy

The design for this study included drawing search terms from the literature to find the most relevant articles and books to the topic. The starting point for key searches is the University of Oregon library. Numerous databases and search engines are used to discover relevant documents and weed out articles that do not meet the needs of this paper. Search results are recorded in a table format for documenting the success rate of each database or search engine as well as each term is evaluated for success at finding relevant articles.

Search terms.

Search terms are helpful for finding appropriate research from databases and search engines (Leedy & Ormrod, 2005). These key terms are based on the most common usage, identified within the preliminary examination of literature for this study. The following search terms are used:

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:Bold, Italic

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:Bold

Computer forensics

Electronic crimes

Computer fraud

Fraud investigations

Sarbanes-Oxley

Information security

Security policy

Search engines and databases

Google Scholar, WorldCat, Academic Search Premier ACM Digital Library provide the best results from all of the searches (see Appendix A for search report). Other indexes used include OneSearch, CiteSeer, Computing Research Repository and LexisNexis

jmullis 6/4/09 6:29 PM
Deleted: Move the table to Appendix A.

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font color: Auto

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font color: Auto

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font color: Auto

Academic. Results are based on relevancy criteria including author credentials, date published and juried or non-juried, as a way to find the best articles and weed out non-relevant documents. The most important factor is if the research focuses on one or more of the key components of the research study, including Sarbanes-Oxley, computer forensics or publicly traded company security policy.

Documentation Approach

Once all of the literature is collected, it is filed into computer folders that are titled by the major areas of inquiry of this study. Sub-section folders are added to separate the texts into smaller groups and make retrieval easier. A Microsoft Word document stores a working copy of the reference list and history or recorded searches and is added to the draft of this study when any changes are made. References and notes for the study are documented using Microsoft Excel in order to better organization of the data. Search term records are entered into tables using Microsoft Word. This method formats the search record in a way that allows information to be organized and any pertinent data found quickly.

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font color: Auto
jmullis 6/4/09 6:29 PM
Deleted: gives

Data Analysis Plan

This study uses the data analysis spiral method to support data analysis (Leedy & Ormond, 2005) to ensure all important content is examined and noted. The spiral approach comprises of 4 steps including organization, perusal, classification, and synthesis (Leedy & Ormond, 2005). The organization step of the spiral consists of filing the information and breaking down found categories into smaller groups. Perusal includes reading the material to get a better sense of content and noting any interpretations (Leedy & Ormond, 2005). The classification step of the spiral is a repetitive process which helps find meanings in the data. In the synthesis step, tables

are created based on the preliminary larger groupings a) Computer forensics, b) Publicly traded companies, and c) the impact of Sarbanes-Oxley in relation to collection and maintenance of relevant evidence. For inclusion in this study, each resource will have at least two of the three key groupings mentioned.

Literature collected for data analysis is analyzed using the conceptual analysis method (Busch et al., 2005) in order to determine if the chosen literature discusses areas of inquiry relevant to this study (Busch et al., 2005). This method provides a process of steps to design an approach to coding selected literature based on specific criteria determined by the researcher (Busch et al., 2005). The eight steps in conceptual analysis include:

1. Level of analysis. Focus is on certain terms, sets, or phrases or words that makeup the concept that is analyzed. The objective of the data analysis process is to discover factors related to these larger concepts:

- Computer forensics
- Collection and maintenance of relevant evidence
- Publicly traded companies
- Sarbanes-Oxley

2. How many concepts. The relevant concepts of focus in the coding process include some flexibility to enable relevant, but unanticipated, concepts to emerge. The initial coded concepts are:

- Forensics
- Governance
- Electronic crime

- Fraud
- Records
- Information security
- Compliance
- Record(s) and Record keeping
- Relevant evidence

3. Code for existence or frequency of a concept. The data will be coded for existence in order to give a better idea of the relevancy for this study. Particular attention is paid to concepts and themes found in the literature instead of terms found. Concepts are important to finding the most relevant material for review, as they point to common themes and not just repeated terms.

4. Distinguish among concepts. Concepts will be generalized to accommodate for words that have the similar meaning or implication, for example, ‘record’ and ‘records’ and ‘record keeping’. Concepts that are not similar will be separated and their own coding applied. Terms within the concept relating to electronic crime include fraud and evidence but do not include abuse, which could be improper but not criminal.

5. Rules for coding. Rules are helpful in keeping the results valid and coherent through the process. This allows for consistently coding the same way each time. For the purposes of this study, similar terms including computer forensics and data forensics are coded as the same term.

6. Irrelevant information. Information deemed irrelevant is used to examine the concepts to find any changes that can strengthen the research. Most irrelevant words will be ignored unless the words can impact the already selected concepts.

7. Code the text. Coding for this study is accomplished manually by reading each work and writing down any occurrences of concepts or themes. Each reference selected for use in the data

set is initially manually coded using index cards and then the data is entered into a table in Microsoft Word. This table includes the author, terms, frequency of term, page numbers for found terms, and a remark on relevancy to this study. The code table is presented in Appendix B.

8. Analyze results. Conclusions are drawn from the data and irrelevant information is discarded. The data is limited to the concepts predetermined in the early stages of the process, making concept choices important to the overall success of the study.

After coding and analysis are completed, conclusions are drawn from the data (Busch, 2005). The Writing Plan explains how the Review of Literature section is structured and developed.

Writing Plan

After coding and analysis, the Review of the Literature section of the document is written using a thematic approach (UNC, 2007). Thematic reviews are good for organizing data collected and focus on topics rather than time progression (UNC, 2007). The review does not focus on the chronological history of Sarbanes-Oxley, but instead on the themes found in the data. The final set of themes is determined by examining the results of the coding process described above, and making comparisons to a set of three pre-selected areas of inquiry including: a) computer forensics procedures, b) publicly held security policies, and c) the impact of Sarbanes-Oxley. Anticipated themes for each area follow:

Computer forensic procedures. How procedures are determined in the wake of new regulation such as Sarbanes-Oxley in order to prevent and detect corporate fraud, computer abuse and other criminal activity. Anticipated themes within computer forensics include training

for compliance with applicable laws and planning correct procedures to deal with alleged improper activity.

Publicly held companies. The specific issues that are important for public corporations compared to private companies related to computer forensics and Sarbanes-Oxley. Anticipated themes include record retention and destruction of electronic data inside of the compliance with federal law.

Impact of Sarbanes-Oxley. How Sarbanes-Oxley impacts computer forensics activities as well as security policy within public companies, specifically related to develop record keeping and destruction of electronic records policies in relation to collection and maintenance of relevant evidence.

jmullis 6/4/09 6:26 PM
Deleted: Adequate (once research question is further examined)

Annotated Bibliography

The annotated bibliography consists of the most relevant research selected for this study. Annotations include abstracts derived directly from each source. The bibliography contains 20 items, including articles and books, which have been chosen from hundreds of options from the collected literature in this project, based on evaluation criteria. The following items form the group of references (data set) subjected to content analysis. As such, they all contribute to the content presented in the Review of References and Conclusion sections of the paper. Credibility for the selected literature is based on a critical evaluation of each item using portions of Smith's (2008) criteria including authority, currency, quality, and relevance this study.

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font color: Auto

Anastasi, J. (2003). ***The new forensics: Investigating corporate fraud and the theft of intellectual property*****. Hoboken, N.J.: John Wiley & Sons.**

Abstract: An in-depth look at the tools, techniques, and tactics used in computer forensics The New Forensics introduces readers to the world of business forensics, using interesting vignettes, interviews, and actual crime reports. It examines recent cases in which the use of computer forensics led to evidence linking executives to fraud and covers issues such as the theft of trade secrets, the use of data mining, money laundering, and other types of theft and fraud. Author Joe Anastasi, a well-respected leader in computer and business forensics, leads the reader on a shadowy journey through top-secret government offices and real-life business investigations while covering the moral and legal issues surrounding corporate crime.

Comment: This article identifies real case examples of corporate computer forensics activities and discusses current topics. The book also covers cases involving Sarbanes-Oxley and adds factors that contribute to development of several themes in this study. The author is credible

based on his over 33 years of experience in the field including working as Global Leader for one of the largest computer forensics practices in the world, Deloitte and Touche. He is also a Diplomate Member of the American College of Forensic Examiners.

Barker, R., Cobb, A., & Karcher, J. (2009). The legal implications of electronic document retention: Changing the rules. *Business Horizons -Bloomington. 52*(2), 177-186.

Abstract: Document retention policies are an often overlooked aspect of information management in most organizations. As 99% of business documents are currently being produced electronically, processes governing the location and storage duration of these documents are very important. Given that most organizations in the United States will find themselves named in a lawsuit and the documents mentioned above may have to be produced in original form for litigants during discovery, document retention policies can spell the difference between successful defense and painful, expensive loss in litigation. This article explores the new rules for electronic discovery and how those rules should drive changes regarding organizational management and storage of documents.

Comment: This article has relevancy and adds value to this study by examining the impact of Sarbanes-Oxley in relation to policies for record retention. This paper also looks at electronic record management in relation to computer forensics. The authors are professors at the University of Louisville and Dr. Cobb runs a computer forensic consultancy. This paper is published in a peer-reviewed journal, *Business Horizons*.

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:(Default) Times New Roman

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:(Default) Times New Roman

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:(Default) Times New Roman

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:(Default) Times New Roman, Italic

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:(Default) Times New Roman

Bassett, R., Bass, L., & O'Brien, P., (2006). Computer forensics: An essential ingredient for cyber security. ***Journal of Information Science and Technology*****, August 2006. Retrieved April 4, 2009, from http://www.jist.info/volumes/vol3/vol3is1/vol3is1-2.pdf**

Abstract: Computer forensics uses computer investigation and analysis techniques to collect evidence regarding what happened on a computer that is admissible in a court of law. Computer forensics requires a well balanced combination of technical skills, legal acumen, and ethical conduct. Computer forensics specialists use powerful software tools to uncover data to be sorted through, and then must figure out the important facts and how to properly present them in a court of law. Cyber crime rates are accelerating
and computer forensics is the crucial discipline that has the power to impede the progress of these cyber criminals.

Comment: This article discusses major themes examined in this study including electronic evidence, legal issues involving corporate records, and publicly held corporations. This article is relevant due to the topic of investigative strategies and security policy and the recent publication date in 2006. Credibility is determined by the fact that the article is published in a peer-reviewed journal. Additionally, Dr. Bassett is the Assistant Dean for the Ancell School of Business at Western Connecticut State University and his co-authors are students in the school.

Bendarx, A. (2005). Compliance: Thinking outside the Sarbox. ***Network World*****, February 2005. Retrieved April 4, 2009, from http://www.networkworld.com/research/2005/020705sox.html**

Abstract: This article describes the sections of Sarbanes-Oxley that impact corporate IT departments and the major hurdles that corporations must go through in order to comply with the legislation. The authors give examples from several companies including Qualcomm, Quadramed, Citrix Systems, and ADP. The complex nature of Sarbanes-Oxley compliance and the demands put on IT departments are also discussed.

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:(Default) Times New Roman

Comment: This article is relevant to this study because it examines themes such as Sarbanes-Oxley and corporate information security. The author is an associate editor for Network World and has written or edited hundreds computer security related articles. Network World is a trade publication that focuses on network security and the themes related to this study.

Carrier, B. (2002). *Open Source Digital Forensics Tools: The Legal Argument.*

Retrieved April 4, 2009, from

http://www.atstake.com/research/reports/acrobat/atstake_opensource_forensics.pdf

Abstract: This paper addresses digital forensic analysis tools and their use in a legal setting. To enter scientific evidence into a United States court, a tool must be reliable and relevant. The reliability of evidence is tested by applying "Daubert" guidelines. To date, there have been few legal challenges to digital evidence, but as the field matures this will likely change. This paper examines the Daubert guidelines and shows that open source tools may more clearly and comprehensively meet the guidelines than closed source tools.

Comment: This article discusses the major theme of computer forensics and the legal implications of examining evidence. This article is relevant due to the topic of investigative strategies and the handling of electronic evidence. The author publishes in the area of forensic

software tools. He is a well known expert in the field and is member of several computer forensic committees including the Digital Forensic Research Workshop.

Kovacich, G. (1999). Introduction to Computer Fraud -- Part 1. *Computer Fraud and Security. 1999*(7), 12-17.

Abstract: We sometimes get so involved in the details and technicalities of a topic that we often make it more complicated than it is. Computer fraud is just such a topic. So, every once in a while, we should go back to the basics, the baseline. By doing so, it is hoped that this will help ensure that our anti-fraud programs are focused on the right targets and have the right objectives. To successfully deal with computer fraud, one must understand our information age, global business environment, what is meant by computer fraud, who and what are the threats, and how to mitigate those threats.

Comment: This paper examines several key themes of this study including computer forensics principles and threats from employees using electronic means inside corporations. The definition and history of computer fraud are discussed in addition to specific examples of employee profiles that are threats to electronic records. The author has over 40 years of computer security experience and holds a Ph.D. in criminology. In addition to previously holding security consultant positions, the author was a lecturer for undergraduate and graduate courses in technology crime investigations.

Kruse, W., & Heiser, J. (2001). *Computer forensics: Incident response essentials*. Boston: Addison-Wesley.

Abstract: Written by two experts in digital investigation, *Computer Forensics* provides

extensive information on how to handle the computer as evidence. Kruse and Heiser walk the student through the complete forensics process from the initial collection of evidence through the final report. Topics include an overview of the forensic relevance of encryption, the examination of digital evidence for clues, and the most effective way to present your evidence and conclusions in court. Unique forensic issues associated with both the Unix and the Windows NT/2000 operating systems are thoroughly covered.

Comment: This book discusses the major theme of computer forensics as well as covering security policy implications relating to computer forensics. This article is relevant due to the topic of computer forensics procedures, investigative strategies and the handling of electronic evidence. The author is a computer forensic expert witness in court, instructor and serves as Vice President of Encore Discovery Solutions, a global electronic discovery company.

Mandia, K., Prosise, C. & Pepe, M. (2003). ***Incident response & computer forensics*****.**

New York: McGraw-Hill/Osborne.

Abstract: *Incident response & computer forensics* is a guide for responding to computer forensic incidents on Windows and Unix operating systems. The book defines incident response and computer forensics as well as gives case examples of actual incidents. A chapter on handling corporate evidence, a chapter on data storage related to computer forensics, and numerous real-world cases are examined. Legal issues and procedures are examined in live examinations for analyzing attacks or crimes that are in progress.

Comment: This book is a resource for staff that are responsible for incident handling in computer incidents. The book examines data storage, record retention and evidence in electronic crime. The book specifies how to prepare for security incidents and establish security policy. The

authors are viewed as experts in computer forensics and computer security because they have been involved in hundreds of computer forensics cases.

Marcella, A., & Menendez, D. (2008). ***Cyber forensics: A field manual for collecting, examining, and preserving evidence of computer crimes*****. New York: Auerbach Publications.**

Abstract: Given our increasing dependency on computing technology in daily business processes, and the growing opportunity to use engineering technologies to engage in illegal, unauthorized, and unethical acts aimed at corporate infrastructure, every organization is at risk. Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes provides a comprehensive, highly usable, and clearly organized resource to the issues, tools, and control techniques needed to successfully investigate illegal activities perpetuated through the use of information technology. Traditional forensics professionals use fingerprints, DNA typing, and ballistics analysis to make their case. Infosec professionals have to develop new tools for collecting, examining, and evaluating data in an effort to establish intent, culpability, motive, means, methods and loss resulting from e-crimes. The field bible for infosec professionals, this book introduces you to the broad field of cyber forensics and presents the various tools and techniques designed to maintain control over your organization.

Comment: This book is relevant for this study because it directly relates to computer forensics and examining electronic evidence. The book also covers the area of security policy in relation to computer forensics and the need for careful planning for security issues. The editors are credible based on years of professional experience and academic achievements. Dr. Marcella is a security consultant and professor at Webster University. He has authored or edited 25 books on IT

security and auditing. Mr. Menendez has over 25 years of professional experience as an IT auditor and has an MBA from Saint Louis University.

Muller, G., Sackmann, S., & Prokein, O. (2006). IT-Security: New Requirements, Regulations and Approaches. *Handbook on Information Technology in Finance*. Springer. Retrieved April 4, 2009, from http://www.springerlink.com/content/r223w381t22p6305/fulltext.pdf

Abstract: Over the past decades, the business environment in the banking sector has changed substantially. Financial service providers and direct brokers have entered the market for private customers. Insurances meanwhile offer investment funds and other products for retirement provision and companies that usually operate in other branches offer new services to customers (e. g. home-banking software of Microsoft). Faced with such increased competition, banks, in particular, pursued Customer Relationship Management (CRM) (Sackmann and Strüker 2005) as a strategy for canvassing new customers and optimizing existing customer relationships. This personalization has a serious side effect: the business of whole institutions depends on the availability, correctness and security of the infrastructure to run the services. Security and the relationship between customers and providers has become a critical issue for both to protect assets and to provide transparency.

Comment: This article discusses the major theme of security policy and the impact of Sarbanes-Oxley Act. This article is relevant due to the topic of security policy and the impact of Sarbanes-Oxley on corporations. The authors are all professors who have published multiple times in peer-reviewed journals, including the *Handbook on Information Technology in Finance and Business*, *Journal of Grid Computing*, and *Information Systems Engineering.*

Nelson, B., Phillips, A., Enfinger, F., & Steuart, C. (2006). *Computer forensics and investigations* (2nd ed.). Boston: Thomson/Course Technology.

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:Not Italic

Abstract: "Computer Forensics and Investigations" offers a solid introduction to a field that is vitally important. With the continued growth of the Internet and the increase in the use of computers worldwide, computers are being used to commit crimes with more frequency. Computers also make it possible to record crimes, including records of embezzlement, e-mail harassment, leaks of proprietary information, and even terrorism. Law enforcement, network administrators, attorneys, and private investigators now rely on the skills of professional computer forensics experts to investigate criminal and civil cases. "Computer Forensics and Investigations" is intended for novices who have a firm understanding of the basics of computers and networking. It can be used to help you pass the appropriate certification exams and covers multiple operating systems as well as a range of computer hardware. "Computer Forensics and Investigations" is your guide to becoming a skilled computer forensics investigator.

Comment: This book examines relevant themes in this study including computer forensics, evidence handling, and electronic crime. The book discusses evidence collection and best practices for establishing policies to prevent computer abuse and crime. The book is targeted for readers with little or no experience with computer forensics but would like to understand the process of collecting and analyzing computer data. The authors are credible based on their work and academic experience. Amelia Phillips, a graduate of the Massachusetts Institute of Technology and a Fulbright Scholar, has over 20 years of professional computer security experience. Bill Nelson has over six years of computer forensics investigation experience with a Fortune 50 corporation and has authored several forensic books and articles. Frank Enfinger is a faculty member at North Seattle Community College and works as a Computer forensics

specialist for a police department. Christopher Steuart is an attorney specializing in computer forensics and was a former information security officer with a Fortune 50 corporation.

Nolan, R., O'Sullivan, C., Branson, J., & Waits, C. (2005). ***First responders guide to computer forensics*****. Retrieved April 4, 2009, from www.cert.org/archive/pdf/FRGCF_v1.3.pdf**

Abstract: This handbook is for technical staff members charged with administering and securing information systems and networks. It targets a critical training gap in the fields of information security, computer forensics, and incident response: performing basic forensic data collection. The first module describes cyber laws and their impact on incident response. The second module builds understanding of file systems and outlines a best practice methodology for creating a trusted first responder tool kit for investigating potential incidents. The third module reviews some best practices, techniques, and tools for collecting volatile data from live Windows and Linux systems. It also explains the importance of collecting volatile data before it is lost or changed. The fourth module reviews techniques for capturing persistent data in a forensically sound manner and describes the location of common persistent data types.

Comment: This paper is a resource for responders to information security incidents and is relevant to this study because it covers computer forensic techniques, evidence handling procedures and contains information regarding legal issues within investigations of corporate incidents. The paper is written by a professional organization that provides information for experienced security personnel in the best practices of computer forensics based on legal and technical research in the field. Sarbanes-Oxley and other laws that impact the collection of electronic evidence are discussed as well as case law involving computer forensics. The authors

have many years of academic and professional experience that make them credible for inclusion in this study. The authors are part of Carnegie Mellon University's Computer Emergency Response Team (CERT). CERT is a federally funded research program that is a communication and coordination center for incidents that involve computer security. The research includes computer forensic incident handling and prevention of major internet crimes.

Rantala, R. (2008). *Cybercrime against business*. Bureau of Justice Statistics. Retrieved April 2, 2009, from http://www.ojp.usdoj.gov/bjs/pub/pdf/cb05.pdf

Abstract: Presents the nature and prevalence of computer security incidents among 7,818 businesses in 2005. This is the first report to provide data on monetary loss and system downtime resulting from cyber incidents. It examines details on types of offenders, reporting of incidents to law enforcement, reasons for not reporting incidents, types of systems affected, and the most common security vulnerabilities. The report also compares in-house security to outsourced security in terms of prevalence of cyber attacks. Appendix tables include industry-level findings.

Comment: This publication discusses and presents statistical information on electronic crimes and discusses the comparison of internal security versus external security. This study examines internal corporate records and computer forensics activities and Rantala's statistics are relevant. The author is a statistician and program manager for the Department of Justice Bureau of Statistics (USDOJ/JBS). The USDOJ/JBS publishes crime reporting and is authorized by Federal law.

Richardson, S. (2005). ***Compliance and computer forensics.*** **Retrieved April 2, 2009, from http://toorcon.techpathways.com/uploads/ComplianceAndComputerForensicsWhitePaper09-05.pdf**

Abstract: Information security compliance requires the precise enforcement of policies and controls. Digital investigations utilizing computer forensics are an essential part of this enforcement. This white paper reviews key information security laws and regulations that mandate computer forensics for compliance.

Comment: The paper examines important aspects that directly relate to this study. The paper examines Sarbanes-Oxley, computer forensics, records management in relation to electronic evidence. The author has over 25 years of management experience in computer companies. He holds a BA in electrical engineering from MIT and an MBA from Harvard Business School.

Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745. Retrieved April 1, 2009, from http://www.sec.gov/about/laws/soa2002.pdf

Abstract: The Sarbanes-Oxley statute is legislation that attempts to help prevent corporate fraud. The law was enacted after a series of large accounting fraud cases occurred including Enron, WorldCom and Tyco International. Sarbanes-Oxley required the creation of a Public Company Accounting Oversights Board (PCAOB) to monitor and regulate auditing firms that audit publicly held corporations. The PCAOB acts as the enforcement arm for Sarbanes-Oxley and handles inspections, investigations and disciplinary boards in Sarbanes-Oxley cases. Sarbanes-Oxley's main provisions include certification of accurate conditions of the company's financials, establishing internal controls, and establishes punishments for destruction of records. The Act

also introduces whistleblower protection for employees and potential punishment for punishing whistleblowers.

Comment: This law is the key to this study and changes the way public companies have to respond to computer incidents. The law is important for this study as it also changes the way companies are required to store electronic information and how it will destroy data. The main authors of the law are Mike Oxley and Paul Sarbanes, both congressmen with over 60 years in political office. Paul Sarbanes was the longest serving senator in Maryland's history and both finished their political careers in 2007.

Small, M. (2009). The root of the problem - malice, misuse or mistake? *Computer Fraud and Security. 2009*(1), 6-9.

Abstract: Organizations worldwide rely on business-critical information systems to run their businesses, yet a major loophole for many of these systems is the administrator account. Much has been made of the threat of external hackers who cause security breaches in organizations. Although this is a real problem, the insiders in an organization may be responsible for as many security breaches as external hackers. In addition, not only malice but also mistakes and misuse by employees are an important reason for loss of vital services. How can organizations protect themselves from these problems?

Comment: This article takes a closer look at internal threats to electronic records by employees. The author looks at techniques for creating a security policy and minimizing damage from internal attacks. Themes that indicate a relevance to this study examined in this article include computer forensics, computer fraud, and security policies. The author is a principal security

consultant and strategist for Computer Associates, one of the world's largest IT software providers.

Steel, C. (2006). ***Windows forensics: The field guide for conducting corporate computer investigations*****. Indianapolis, IN: Wiley Pub.**

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:(Default) Times New Roman

Abstract: An arcane pursuit a decade ago, forensic science today is a household term. And while the computer forensic analyst may not lead as exciting a life as TV's CSIs do, he or she relies just as heavily on scientific principles and just as surely solves crime. Whether you are contemplating a career in this growing field or are already an analyst in a Unix/Linux environment, this book prepares you to combat computer crime in the Windows world. Here are the tools to help you recover sabotaged files, track down the source of threatening e-mails, investigate industrial espionage, and expose computer criminals.

Comment: This book is a guide for computer forensics and focuses on Windows forensics. The guide discusses handling evidence and investigations of electronic crimes within a corporate setting. The examination of electronic evidence and corporate crime and abuse make this book relevant to this study. The author is an adjunct professor and has investigated more than 300 security incidents over the course of his career. He is a PhD candidate and a consultant in computer forensics for public and private sector organizations.

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:(Default) Times New Roman

Vacca, J. R. (2005). ***Computer forensics: Computer crime scene investigation*****. Hingham, MA: Charles River Media.**

Abstract: Organizations today face an ever-growing threat of cyber crime and security violations. These attacks can occur internally as well as from an external source and include

fraud, copyright infringement, and stolen data. Computer Forensics: Computer Crime Scene Investigation, Third Edition provides a comprehensive introduction to computer forensics investigative techniques. The reader will gain the knowledge and skills required to conduct a computer forensics investigation from initial discovery to completion. The reader will also learn how to exploit their organization's Computer Incident Response Team (CIRT); collect, manage and record digital evidence; and leverage powerful software tools and techniques to uncover hidden or deleted information. Approximately 25% of the book is dedicated to hands-on exercises. Employing the latest software forensic tools contained in the CD in the back of the book, users will be able to capture disk images, undelete files, search memory in real-time for hidden data, and discover compromised machines. Much has changed in the realm of information security and computer forensics since the previous edition, so the book has been completely updated to cover advances in the field.

Comment: This book focuses on the steps to take in responding to computer incidents. In relation to this study, the book covers evidence handling and how to access and investigate electronic evidence. The author has written over 60 computer-related books and holds two Master's degrees. The book meets the criteria for inclusion in this study because of authority, currency, relevance and quality.

Volonino, L. (2003). Electronic evidence and computer forensics. *Communication of the Association for Information Systems*. Retrieved April 27, 2009, from http://cais.isworld.org/articles/12-27/article.pdf

Abstract: Information and communication systems are now breeding grounds for electronic-evidence (e-evidence) in audits, investigations, or litigation. Increasingly organizations are being

ordered by law or lawsuit to preserve, retrieve, and hand-over relevant electronic records (e-records) because "the courts are uniformly recognizing the discoverability of electronic communication and documents" [Nimsger & Lange, 2002]. This trend is an outgrowth of aggressive tactics by regulators to ensure corporate accountability and deter fraud.

Comment: This paper covers records management and computer forensics, specifically discussing themes that are the basis for this study. These themes include handling electronic evidence and aspects of records management in a corporate setting. The paper examines how Sarbanes-Oxley impacts records management and policy decisions. The author is a professor at Canisius College and computer forensic consultant that has authored numerous books and journal articles.

Wolfe, H. (2007). Electronic forensics: A case for first responders. ***Proceedings of Forum for Incident Response and Security Teams (FIRST) 2007. Seville, Spain*****. Retrieved April 27, 2009, from http://www.first.org/conference/2007/papers/wolfe-henry-paper.pdf**

Abstract: Almost every aspect of our lives is touched or somehow controlled by technology driven processes, procedures and devices. It is therefore important to understand that because of this pervasive electronic influence, there is a high probability that a successful criminal or unacceptable incident will occur within the perimeter of an organization’s information and/or computer and network infrastructure. The difference between conducting a successful investigation resulting in a potential prosecution or failing these will often lie squarely in the lap of the electronic forensic investigator. If potential evidence is compromised at any point in the investigation, it will be unacceptable in a court of law. The highest risk of compromise occurs at

the point prior to evidentiary acquisition. The first responder's primary responsibility is to protect and preserve potential evidence and to see to it that suspect electronic devices and storage media are not tampered with by anyone until such time as the professional electronic forensics investigator (law enforcement or private) takes full control of the scene. This paper will explore electronic forensics demonstrating the need and making the case for the appointment and training of a first responder to incidents where electronic devices may have been used.

Comment: This paper discusses the several aspects of the themes that are the basis of this study including policy development regarding computer forensics. This article is relevant due to the topic of computer forensics procedures and how to set policies for those that respond to computer incidents. The author has over 50 years of professional experience in the computer industry and a frequent speaker on the topic of computer forensics. He is a professor at the University of Otago in New Zealand and a security consultant for governmental organizations worldwide.

Review of the Literature

In response to a series of corporate financial scandals, Congress enacted the Sarbanes-Oxley Act in 2002. The Act is organized into eleven sections, called Titles. Sarbanes-Oxley aims to increase accounting oversight and corporate responsibility by enhancing disclosure requirements, increasing accountability, creating new federal criminal penalties, and increasing penalties for current financial crimes.

In several Titles, Sarbanes-Oxley attempts to address the issues developing around the increase of electronic records produced in corporate environments. As the amount of electronic records that are produced increases, so does the amount of electronic evidence that must be accounted for during computer forensic incidents. Corporations are now compelled to address record retention and potential legal burdens associated with electronic documents.

Theme #1: How Sarbanes-Oxley Changes Computer Forensic Procedures in Publicly Held Companies

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:Bold

To better understand how Sarbanes-Oxley affects computer forensics, a closer look at section 404 of the act is necessary. Section 404 states that a corporation should assess the how effective their internal controls are and annually report this effectiveness statement to the Security and Exchange Commission (SEC). The assessment must also be externally reviewed by an outside auditor. Section 404 is significant in that a large amount of resources are needed for compliance

Mike A Pritchard 5/21/09 9:25 PM
Formatted: Bullets and Numbering

and a greater number of records are required to be stored. Section 404 indirectly forces the ***closer inspection of information security controls*** for Sarbanes-Oxley compliance.

Largely due to the increased scrutiny of electronic records in Sarbanes-Oxley, corporations must have a plan in place to ***respond to incidents that involve computer forensic analysis of records***. Personnel who are given responsibility for incident response should be well trained and prepared for handling electronic records (Richardson, 2005). In-house response teams should be able to handle the compliance issues for Sarbanes-Oxley and outside computer forensic consultants should be used in cases of suspected internal employee criminal activity (Richardson, 2005).

Sarbanes-Oxley directly impacts ***corporate electronic records management***. The impact of Sarbanes-Oxley on electronic records management largely consists of two components. The first component that is spelled out in Section 802 places criminal liability on the destruction of records concerning a federal investigation or bankruptcy. Sarbanes-Oxley also ***prohibits employees from altering or destroying records***. Section 802 also ***prohibits tampering with witnesses or whistleblowers*** in the course of an investigation (Sarbanes-Oxley Act, 2002). To fully comply with Sarbanes-Oxley, policies concerning the corporation's procedures for retention of records, destruction of records and response to incidents must be shown to employees and auditors.

Section 404 of Sarbanes-Oxley requires corporations to ***initiate and provide an effective internal control system***. Under Sarbanes-Oxley rules, internal controls must provide assurance that

corporate assets are used and disposed within the internal control structure that complies fully with Sarbanes-Oxley.

Section 302 of Sarbanes-Oxley states that the Chief Executive Officer (CEO) and Chief Financial Officer (CFO) are responsible for setting internal controls. Section 302 also requires executives to evaluate the company's internal controls and their effectiveness. Executives are required to assess controls ability to prevent and detect corporate fraud.
Any deficiencies discovered in internal control policy by executives must be reported including the controls design or operation. Sarbanes-Oxley holds senior executives of public companies and specifically requires reporting to be clear and demonstrable information regarding the corporate internal control (Sarbanes-Oxley Act, 2002).

Section 409 of Sarbanes-Oxley sets a requirement for ***timely communication on material changes with financial or operational conditions***. In order for compliance with the intent of Sarbanes-Oxley, this communication should be current and rapidly communicated to the public. In order to comply and communicate changes in the corporation's conditions, internal controls should be designed with Sarbanes-Oxley's section 409 in mind.

Failure to investigate internal employee complaints quickly and within Sarbanes-Oxley guidelines can imply absence of internal controls stated under Section 404 and possibly violate section 302 which requires immediate fraud disclosure. Additionally, Section 802 of SOX outlines the criminal penalties for destruction of electronic records (Sarbanes-Oxley Act, 2002).

Section 806 of Sarbanes-Oxley provides ***protection for any employee who is retaliated against for whistle blowing*** if employee believes fraud is occurring within the corporation. This protection covers employees that feel improper activities are occurring or fraudulent activities are taking place and allows them to alert authorities without fear of reprisal from the corporation.

Section 802 of Sarbanes-Oxley is also likely to have an impact on how public corporations handle electronic records. Section 802 references the processes of electronic records retention and how records are created, sent, or received in relation to audits and reviews. This provision could require many public corporations to retain more records than before the enactment of Sarbanes-Oxley (Sarbanes-Oxley Act, 2002).

For compliance with the provisions of Sarbanes-Oxley, corporations must ***consider electronic records when determining what should records will be retained*** and what records should be destroyed. Corporations must consider Sarbanes-Oxley compliance when developing computer forensics procedures in order to respond to incidents in a manner that protects potential evidence (Richardson, 2005). The deletion, whether intentional or not, of electronic records is considered a serious matter under Sarbanes-Oxley. These important events require immediate response and communication to the public and shareholders. As more records are electronic and require specialized software and training to respond to incidents, computer forensics practices become more important to determining the circumstances of a record deletion.

Now corporations need to learn from previous failures that led up to Sarbanes-Oxley and implement computer forensic investigations immediately when incidents occur. The response

structure created by a corporation will help preserve electronic evidence and recover significant deleted records. Computer forensic tools can help alleviate permanent loss of data required in Sarbanes-Oxley investigations and assist in establishing if the destruction or deletion was the result of authorized action on the part of employees in the corporation.

Theme #2: How Sarbanes-Oxley Impacts Records Retention in Publicly Held Companies

jmullis 6/4/09 5:12 PM
Deleted: *Theme #2: Organizational culture*

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:Bold, Italic, Font color:

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:Bold, Italic, Font color:

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:Bold, Italic, Font color:

Mike A Pritchard 5/21/09 9:25 PM
Formatted: Bullets and Numbering

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:Bold

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:Not Bold

Public corporate IT departments must have policies in place to comply with Sarbanes-Oxley, including suitable record retention and destruction, and information security. Corporate managers must understand the requirements described in the law and make sure appropriate policies are in put in to place (Wolfe, 2007). Section 802 of Sarbanes-Oxley states that anyone who destroys or alters records can be fined up to $5 million and jailed of up to 20 years.

Section 802 directs public corporations to preserve corporate audit records for a five year period and to disseminate any rules relating to the retention of relevant records from an audit within 180 days. This section states that those violating the new stipulations may be imposed with large fines and/or long jail terms (Sarbanes-Oxley Act, 2002). Section 802 also prohibits tampering with witnesses or whistleblowers in the course of an investigation.

Public corporations are beginning to understand the necessity of computer forensics procedures underneath the rules of Sarbanes-Oxley (Richardson, 2005). Because computer forensics has been determined as the preferred method for determining if records have been deleted or altered, forensic procedures are critical for compliance with Section 802 (Richardson, 2005). Electronic

record retention and destruction policies can reduce costs when information retrieval time is reduced (Volonino, 2003). In addition to reducing costs, proper management of electronic records can save the company legal difficulties when policies align with Sarbanes-Oxley specifications (Volonino, 2003).

Records retention is an important factor of Sarbanes-Oxley with which most corporations must comply. A record retention policy determines the length of time before records can be destroyed (Barker, 2009). Sarbanes-Oxley implemented new strict records for keeping records available when corporations are reviewed or investigated. Policies should be developed using Sarbanes-Oxley as a guide, specifically Section 802 (Sarbanes-Oxley Act, 2002).

The majority of the records retention policy must include procedures for organization, determining retention periods, and setting the retention schedule for various electronic records. The volume of electronic documents continues to expand and this adds to the pool of potential electronic records needed for legal incidents. If records must be stored for years to comply with Sarbanes-Oxley, the cost and resources needed to maintain these records can become a burden to those responsible (Barker, 2009)

Theme #3: How Sarbanes-Oxley Impacts Internal Security Policies in Publicly Held Companies

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:Bold

Section 404 changes the internal controls of public corporations by requiring new reports and punishment for executive non-involvement. Section 404 requires the management of public companies to produce new reports at the end of every year (Sarbanes-Oxley Act, 2002). These

reports must also be attested to by the independent auditor for the assertion of solid internal controls (Sarbanes-Oxley Act, 2002).

Corporations need to align business operations with the legal requirements of Sarbanes-Oxley, including record retention periods and deletion of records policies. Plans for dealing with audits and investigations should include explaining the potential compliance issues within the constraints of Sarbanes-Oxley. A crucial part of a corporation's plan will include how to respond in the face of an audit or SEC investigation and that destroying records can jeopardize the company.

Section 401 requires full disclosure of any information on the financial status of the company. Most corporations concentrate on Section 404 because it requires that executives attest to the internal control's effectiveness. It requires internal control reports to be created disclosure document referred to as an. An internal control report, which is also included in every annual report, states the internal controls ability to keep the corporation in compliance with Sarbanes-Oxley.

Section 404 addresses the operational compliance of internal controls by requiring that processes and activities must be documented and validated through testing. The provisions of Section 404 provide the public and investors in a corporation with confidence that the processes in records management and internal controls ensure that records and company assets will be protected from improper use. While the Section demonstrates adequate internal controls, it also helps to prevents fraud by requiring documentation of the controls and keeping the executives responsible for the effectiveness of controls.

After the policy is set in motion, companies communicate and document details of the policy and its impact on the corporation (Volonino, 2003). Employees must also be trained on the retention policies and deletion policies of records that include email and files (Volonino, 2003).

Conclusion

The purpose of this literature review is to explore the impact of Sarbanes-Oxley on the development of internal security policies and computer forensics strategies, as these are defined in publicly traded companies. The selected literature utilized in this study reveals that computer forensics plays a key role in relation to mandated compliance with The Sarbanes-Oxley Act of 2002. Computer forensic capabilities include the ability to preserve records, analyze evidence, and hand over to authorities the relevant evidence in a timely manner.

Under Sarbanes-Oxley, executives now are required to sign and acknowledge the accuracy of the reports furnished to the SEC and available to the public. Executives are also required to actively pursue internal controls and test their effectiveness based on the guidelines set forth in the law.

The new requirements make computer forensics a valuable tool in discovery of deleted records and determination of what occurred during incidents. With the heightened Sarbanes-Oxley reporting and controls requirements, corporations may be obliged to increase the level and speed of internal investigations in order to comply.

Sarbanes-Oxley requires that public corporations consider the impact of electronic records in relation to computer forensic procedures. Sarbanes-Oxley imposes new requirements on public corporations and their auditing teams in regard to the retention and destruction of electronic records. Records can no longer be destroyed and must be retained in the event of an investigation. Corporations must follow Sarbanes-Oxley's conditions closely to stay in

compliance. Records must be maintained until they are destroyed, and only destroyed if it is legal to do so.

To protect the corporation from employee wrongdoing in the wake of Sarbanes-Oxley, the corporation must be able to not only preserve electronic records but also quickly respond to incidents. In addition, to be in compliance with Sarbanes-Oxley, corporations must engage in timely reporting. If an incident occurs and an internal investigation starts, forensics must support the provision of correct information to report in the time restraints required by the law. This ability to act quickly and communicate problems to the public and investors would be difficult without the use of computer forensics.

The provisions of Sarbanes-Oxley make it essential that companies develop computer forensics policies and procedures, in order to have the ability to respond to allegations of fraud. In the age of strict regulation such as Sarbanes-Oxley, if a public corporation does not have the policies and procedures in place to collect electronic evidence in a manner that complies with the intent of the law, the corporation risks placing itself in a vulnerable position if audited or investigated.

References

Anastasi, J. (2003). *The new forensics: Investigating corporate fraud and the theft of intellectual property*. Hoboken, NJ: John Wiley & Sons.

Barker, R., Cobb, A., & Karcher, J. (2009). The legal implications of electronic document retention: Changing the rules. *Business Horizons -Bloomington. 52*(2), 177-186.

Bassett, R., Bass, L., & O'Brien, P., (2006). Computer forensics: An essential ingredient for cyber security. *Journal of Information Science and Technology*, August 2006. Retrieved April 4, 2009, from http://www.jist.info/volumes/vol3/vol3is1/vol3is1-2.pdf

Bendarx, A. (2005). Compliance: Thinking outside the Sarbox. *Network World*, February 2005. Retrieved April 4, 2009, from http://www.networkworld.com/research/2005/020705sox.html

Busch, C., De Maret, P., Flynn, T. Kellum, R., Le, S., Meyers, B., et al. (2005). *Content Analysis.* Writing@CSU. Colorado State University Department of English. Retrieved April 27, 2009 from http://writing.colostate.edu/guides/research/content/

Carrier, B. (2002). *Open Source Digital Forensics Tools: The Legal Argument.* Retrieved April 4, 2009, from http://www.atstake.com/research/reports/acrobat/atstake_opensource_forensics.pdf

Cavaliere, F., Mandal, P., & Barnes, C. (2005). Can company e-mail avoid becoming evidence mail? *Proceedings of the 2006 Southwest Decision Sciences Institute.* Retrieved May 20, 2009, from http://www.swdsi.org/swdsi06/Proceedings06/Papers/ISP03.pdf

jmullis 6/4/09 9:49 PM
Deleted:

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:(Default) Times New Roman, Not Bold

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:(Default) Times New Roman, Not Bold

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:(Default) Times New Roman, Not Bold, Italic

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:(Default) Times New Roman, Not Bold

Colorado State Writing Lab (2006). *Steps for conducting conceptual analysis.* Colorado State University. Retrieved April 25, 2009, from http://writing.colostate.edu/guides/research/content/pop3b.cfm

Computer forensics. (2009, April 28). In *Wikipedia, The Free Encyclopedia*. Retrieved April 28, 2009, from http://en.wikipedia.org/w/index.php?title=Computer_forensics&oldid=286557949

Haggerty, J., & Taylor, M. (2006). Managing corporate computer forensics. *Computer Fraud and Security.* 2006 (6), 14-16.

Howell, R., & Cogar, R. (2003). *Record retention and destruction: current best practices. Retrieved* October 25, 2008, from http://www.abanet.org/buslaw/newsletter/0021/materials/recordretention.pdf.

Information technology governance. (2009, May 4). In *Wikipedia, The Free Encyclopedia.* Retrieved May 4, 2009, from http://en.wikipedia.org/w/index.php?title=Information_technology_governance&oldid=287813039

Kissel, R. (Ed.) (2006) *National Institute of Standards and Technology: Glossary of Key Information Security Terms*. Retrieved May 1, 2009 from http://csrc.nist.gov/publications/nistir/NISTIR-7298_Glossary_Key_Infor_Security_Terms.pdf

Kovacich, G. (1999). Introduction to Computer Fraud -- Part 1. *Computer Fraud and Security. 1999*(7), 12-17.

Kruse, W., & Heiser, J. (2001). *Computer forensics: Incident response essentials*. Boston: Addison-Wesley.

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:Not Italic

Leedy, P., & Ormrod, J. (2005). *Practical Research.* Upper Saddle River, NJ: Pearson Education.

Mandia, K., Prosise, C. & Pepe, M. (2003). *Incident response & computer forensics*. New York: McGraw-Hill/Osborne.

Marcella, A., & Menendez, D. (2008). *Cyber forensics: A field manual for collecting, examining, and preserving evidence of computer crimes*. New York: Auerbach Publications.

Meyers, M. and Rogers, M. (2004, Fall). Computer forensics: the need for standardization and certification. *International Journal of Digital Evidence*, *2*.

Muller, G., Sackmann, S., & Prokein, O. (2006). IT-Security: New Requirements, Regulations and Approaches. *Handbook on Information Technology in Finance*. Springer. Retrieved April 4, 2009, from http://www.springerlink.com/content/r223w381t22p6305/fulltext.pdf

National Institute of Standards and Technology. (2007). RBAC & Sarbanes-Oxley Compliance. Retrieved April 4, 2009, from http://csrc.nist.gov/groups/SNS/rbac/sarbanes_oxley.html

Nelson, B., Phillips, A., Enfinger, F., & Steuart, C. (2006). *Computer forensics and investigations* (2nd ed.). Boston: Thomson/Course Technology.

Nolan, R., O'Sullivan, C., Branson, J., & Waits, C. (2005). *First responders guide to computer forensics*. Retrieved April 4, 2009, from www.cert.org/archive/pdf/FRGCF_v1.3.pdf

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:(Default) LKFCBO+TimesNewRoman,Bold, Not Bold, Not Italic, Font color: Black

Obenzinger, H. (2005). *What can a literature review do for me?* Retrieved April 20, 2009, from Stanford University: http://ual.stanford.edu/pdf/uar_literaturereviewhandout.pdf

Patzakis, J. (Spring, 2003). New Accounting Reform Laws Push For Technology-Based Document Retention Practices. *International Journal of Digital Evidence, 2.* Retrieved May 12, 2009, from https://www.utica.edu/academic/institutes/ecii/publications/articles/A065F149-C151-FB73-1E0034E98EB1D145.pdf

Politis, D., Kozyris, P., & Iglezakis, I. (2009). *Socioeconomic and legal implications of electronic intrusion*. Hershey, PA: Information Science Reference.

Rantala, R. (2008).*Cybercrime Against Business*. Bureau of Justice Statistics. Retrieved April 2, 2009, from http://www.ojp.usdoj.gov/bjs/pub/pdf/cb05.pdf

Richardson, S. (2005). *Compliance and computer forensics.* Retrieved April 2, 2009, from http://toorcon.techpathways.com/uploads/ComplianceAndComputerForensicsWhitePaper09-05.pdf

Records management. (2009, April 9). In *Wikipedia, The Free Encyclopedia*. Retrieved May 8, 2009, from http://en.wikipedia.org/w/index.php?title=Records_management&oldid=282853031

Rekhis, S. (2007). Theoretical aspects of digital investigation of security incidents. (CNAS-2008-103). Carthage, Tunisia: The Communication Network and Security Research Laboratory.

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:Not Italic

Rubin, B. (2007). Computer Forensics Foils Financial Data Theft. ISSA Journal August, 2007. Retrieved May 8, 2009, from http://www.mandiant.com/documents/ComputerForensics_ISSAJournal.pdf

Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745. Retrieved April 1, 2009, from http://www.sec.gov/about/laws/soa2002.pdf

Sarbanes-Oxley Act. (2009, April 29). In *Wikipedia, The Free Encyclopedia*. Retrieved, April 27, 2009, from http://en.wikipedia.org/w/index.php?title=Sarbanes-Oxley_Act&oldid=286920978

Seetharaman, A., Senthilvelmurugan, M., & Periyanayagam, R. (2004). Anatomy of computer accounting frauds. *Managerial Auditing Journal. 19*(8), 1055-1072. Retrieved April 27, 2009, from http://theforensicinstitute.org/resources/9_Anatomy_Computer_Accounting_Frauds.pdf

Small, M. (2009). The root of the problem - malice, misuse or mistake? *Computer* Fraud and Security. *2009*(1), 6-9.

Smith, T. (2008). Critical Evaluation of Information Sources. University of Oregon Library. Retrieved May 22, 2009 from http://libweb.uoregon.edu/guides/findarticles/credibility.html

Straub, D. (1990). Effective IS security: An empirical study. *Information Systems Research 1 (3)*: 255-276. Retrieved April 26, 2009, from http://www.cis.gsu.edu/~dstraub/Papers/Resume/Straub1990.pdf

Steel, C. (2006). *Windows forensics: The field guide for conducting corporate computer investigations*. Indianapolis, IN: Wiley Pub.

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:(Default) Times New Roman, Not Bold

Stults, G. (2004). *An Overview of Sarbanes-Oxley for the Information Security Professional*. Sans Institute. Retrieved May 12, 2009, from http://www.sans.org/reading_room/whitepapers/legal/1426.php.

Tipton, H.& Krause, M. (2007). *Information security management handbook*. (ISC)2 Press series, 27. Boca Raton, FL: Auerbach Publications.

UNC. (2007). Literature Reviews. University of North Carolina at Chapel Hill. Retrieved April 29, 2009 from http://www.unc.edu/depts/wcweb/handouts/literature_review.html

United States. (2006, December 1). Federal rules of evidence. Washington, DC: U.S. Government Printing Office. Retrieved April 26, 2009, from http://www.uscourts.gov/rules/Evidence_Rules_2007.pdf

Vacca, J. R. (2005). *Computer forensics: Computer crime scene investigation*. Hingham, MA: Charles River Media.

Volonino, L. (2003). Electronic evidence and computer forensics. *Communication of the Association for Information Systems*. Retrieved April 27, 2009, from http://cais.isworld.org/articles/12-27/article.pdf

Wolfe, H. (2007). Electronic forensics: A case for first responders. *Proceedings of Forum for Incident Response and Security Teams (FIRST) 2007. Seville, Spain*. Retrieved April 27, 2009, from http://www.first.org/conference/2007/papers/wolfe-henry-paper.pdf

Appendix A: Search Results

Search Engine / Database	Terms	Results	Quality
OneSearch Quickset – Law	Computer forensics	9	Poor - few relevant sources
OneSearch Quickset – Law	Electronic crimes	136	Good -many relevant sources
OneSearch Quickset – Law	Computer fraud	51	Good -many relevant sources
OneSearch Quickset – Law	Fraud investigations	87	Good -many relevant sources
OneSearch Quickset – Law	Sarbanes-Oxley	64	Good -many relevant sources
OneSearch Quickset – Law	Information security	1426	Fair - few relevant sources but a large quantity of overall results
OneSearch Quickset – Law	Security policy	144	Poor - few relevant sources – most results were not related to information

			security but national security
OneSearch Quickset – Law	Digital forensics	4	Poor - few relevant sources
OneSearch Quickset – Core Research	Computer forensics	117,309	Fair - few relevant sources but a large quantity of overall results
OneSearch Quickset – Core Research	Electronic crimes	198,696	Fair - few relevant sources but a large quantity of overall results
OneSearch Quickset – Core Research	Computer fraud	123,551	Fair - few relevant sources but a large quantity of overall results
OneSearch Quickset – Core Research	Fraud investigations	92,187	Fair - few relevant sources but a large quantity of overall results
OneSearch Quickset – Core Research	Sarbanes-Oxley	345,964	Fair - relevant sources but a large quantity of overall

			results
OneSearch Quickset – Core Research	Information security	4,301,426	Fair - relevant sources but a large quantity of overall results
OneSearch Quickset – Core Research	Digital forensics	4	Poor - few relevant sources
OneSearch Quickset – Core Research	Security policy	2,673,367	
CiteSeerX	Computer forensics	164	Great - large quantity of relevant sources
CiteSeerX	Electronic crimes	34	Good -many relevant sources
CiteSeerX	Computer fraud	59	Good -many relevant sources
CiteSeerX	Fraud investigations	42	Good -many relevant sources
CiteSeerX	Sarbanes-Oxley	179	Good -many relevant sources
CiteSeerX	Information security	3,386	Fair - few relevant sources but a large quantity of overall

			results
CiteSeerX	Digital forensics	102	Poor - few relevant sources
CiteSeerX	Security policy	6,196	Fair - few relevant sources but a large quantity of overall results
Google Scholar	Computer forensics	4,170	Great - large quantity of relevant sources
Google Scholar	Electronic crimes	629	Good -many relevant sources
Google Scholar	Computer fraud	5,120	Great - large quantity of relevant sources
Google Scholar	Fraud investigations	1,540	Good -many relevant sources
Google Scholar	Security policy	258,000	Great - large quantity of relevant sources
Academic Search Premier	Computer forensics	129	Good -many relevant sources
Academic Search Premier	Electronic crimes	21	Poor - few

			relevant sources
Academic Search Premier	Computer fraud	1209	Great - large quantity of relevant sources
Academic Search Premier	Fraud investigations	715	Good -many relevant sources
Academic Search Premier	Sarbanes-Oxley	1513	Fair - few relevant sources but a large quantity of overall results
Academic Search Premier	Information security	2104	Fair - few relevant sources but a large quantity of overall results
Academic Search Premier	Digital forensics	43	Poor - few relevant sources
Academic Search Premier	Security policy	2,934	Fair - few relevant sources but a large quantity of overall
ACM Digital Library	Computer forensics	1,336	Great - large quantity of relevant sources
ACM Digital Library	Electronic crimes	1,652	Great - large

			quantity of relevant sources
ACM Digital Library	Computer fraud	3,002	Great - large quantity of relevant sources
ACM Digital Library	Fraud investigations	832	Good -many relevant sources
ACM Digital Library	Sarbanes-Oxley	306	Good -many relevant sources
ACM Digital Library	Information security	63,805	Fair - few relevant sources but a large quantity of overall results
ACM Digital Library	HIPAA	443	Good -many relevant sources
ACM Digital Library	Security policy	9750	Good -many relevant sources
Computing Research Repository	Computer forensics	3	Poor - No relevant sources
Computing Research Repository	Electronic crimes	1	Poor - No relevant sources
Computing Research Repository	Computer fraud	1	Poor - No relevant sources

Computing Research Repository	Fraud investigations	0	Poor - No results
Computing Research Repository	Sarbanes-Oxley	4	Poor - No relevant sources
Computing Research Repository	Information security	144	Poor - No relevant sources
Computing Research Repository	HIPAA	0	Poor - No results
Computing Research Repository	Security policy	201	Poor - few relevant sources
LexisNexis Academic	Computer forensics	686	Poor - Articles tended to be from non-technical publications, magazines, newspapers
LexisNexis Academic	Electronic crimes	152	Poor - Articles tended to be from non-technical publications, magazines, newspapers
LexisNexis Academic	Computer fraud	305	Poor - Articles

			tended to be from non-technical publications, magazines, newspapers
LexisNexis Academic	Fraud investigations	1060	Poor - Articles tended to be from non-technical publications, magazines, newspapers
LexisNexis Academic	Sarbanes-Oxley	912	Poor - Articles tended to be from non-technical publications, magazines, newspapers
LexisNexis Academic	Information security	976	Poor - Articles tended to be from non-technical publications, magazines, newspapers

LexisNexis Academic	HIPAA	964	Poor - Articles tended to be from non-technical publications, magazines, newspapers
LexisNexis Academic	Security policy	990	Poor - Articles tended to be from non-technical publications, magazines, newspapers

Appendix B: Frequency of Terms in Data Set

Author	Term(s)	Frequency	Page(s)
Anastasi, J. (2003)	Forensics	29	2, 10, 15, 16, 28, 31, 32, 57, 63, 66, 68, 84, 85, 114, 120, 124, 125, 191, 193, 197, 199, 200, 202, 203, 204, 239, 262, 264, 266
Anastasi, J. (2003)	Sarbanes	0	
Anastasi, J. (2003)	Electronic crime	15	12, 15, 27, 29, 62, 69, 70, 75, 77, 80, 82, 84, 85, 86, 186
Anastasi, J. (2003)	Fraud	26	21, 26, 57, 70, 75, 77, 86, 87, 90, 91, 97, 99,101, 109, 110, 111, 117, 121, 126, 127, 131, 143, 145, 186, 188, 215
Anastasi, J. (2003)	Records	27	14,37,38,39,40,46,47,49,51,59,68,121,139,161,169,170,171,175,176,177,179,181,182,185,192,241,246
Anastasi, J. (2003)	Information security	1	239
Anastasi, J. (2003)	Compliance	1	224
Anastasi, J. (2003)	Record(s) and Record keeping	0	
Anastasi, J. (2003).	Evidence	37	11, 14, 27, 30, 56, 58, 68, 70, 72, 73, 78, 79, 80, 85, 86, 87, 91, 116, 120, 127, 130, 158, 194, 195, 227, 236, 237
Barker, R (2009)	Forensics	2	4, 9
Barker, R (2009)	Sarbanes	0	
Barker, R (2009)	Electronic crime	0	
Barker, R (2009)	Fraud	0	
Barker, R (2009)	Records	6	3, 8
Barker, R (2009)	Information security	0	
Barker, R (2009)	Compliance	3	4, 8, 9
Barker, R	Record(s)	7	6, 7, 9

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:(Default) Times New Roman, Bold

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt

(2009)	and Record keeping		
Barker, R (2009)	Evidence		
Bassett, R (2006)	Forensics	27	1,2,3,4,5,6,7,8,9
Bassett, R (2006)	Sarbanes	0	
Bassett, R (2006)	Electronic crime (cyber crime)	10	1,2,6,7,8,9
Bassett, R (2006)	Fraud	3	7
Bassett, R (2006)	Records	0	
Bassett, R (2006)	Information security	0	
Bassett, R (2006)	Compliance	0	
Bassett, R (2006)	Record(s) and Record keeping	0	
Bassett, R (2006)	Evidence	17	1,2,3,4,5,6,7,8,9
Bendarx, A. (2005)	Forensics	0	online publication, no page numbers
Bendarx, A. (2005)	Sarbanes	6	online publication, no page numbers
Bendarx, A. (2005)	Electronic crime	0	online publication, no page numbers
Bendarx, A. (2005)	Fraud	2	online publication, no page numbers
Bendarx, A. (2005)	Records	0	online publication, no page numbers
Bendarx, A. (2005)	Information security	1	online publication, no page numbers
Bendarx, A. (2005)	Compliance	17	online publication, no page numbers
Bendarx, A. (2005)	Record(s) and Record keeping	0	online publication, no page numbers
Bendarx, A. (2005)	Evidence	0	online publication, no page numbers

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt

Carrier, B. (2002).	Forensics	10	1,2,3,4,6,9
Carrier, B. (2002).	Sarbanes	0	
Carrier, B. (2002).	Electronic crime	3	1,2
Carrier, B. (2002).	Fraud	0	
Carrier, B. (2002).	Records	0	
Carrier, B. (2002).	Information security	0	
Carrier, B. (2002).	Compliance	0	
Carrier, B. (2002).	Record(s) and Record keeping	0	
Carrier, B. (2002).	Evidence	44	1,2,3,7,8,9
Kruse, W (2001)	Forensics	20	2,3,26,59,60,86,115,121,129,133,154,242,253,255
Kruse, W (2001)	Sarbanes	0	
Kruse, W (2001)	Electronic crime	128	1,3,4,6,18,27,28,30,31,32,33,34,38,39,42-44,61,62,104,107,115,116,130,135,136,140,146,150,151,153,154,171,192,193,197-200,211,236,237,238,241,243,269,272,273,275,277-281
Kruse, W (2001)	Fraud	47	2,31,39,42,43,104,171,192,193,200,237,238,269,272,277,282
Kruse, W (2001)	Records	234	29,30,38,43,44,47,61,62,65,66,81,83,85,97,133,150,151-154, 183, 184, 185,186,192,197,207,211,229,230,251,252,270-273,276,278,280-288
Kruse, W (2001)	Information security	10	168,172,185,191,217,227,232,245,
Kruse, W (2001)	Compliance	9	174,205,215,228,229,233,289
Kruse, W (2001)	Record(s) and Record keeping	5	177,183,194,251,293

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt

Kruse, W (2001)	Evidence	434	1-4,18,21,24,25,26,29,32,36,44-48,51,52,56,58-62,69,80,83,84,86,102,104-107,115-121,123-129,140-141,150-153,270-271,288
Mandia, K (2003)	Forensics	27	8,18,22,44,52,68,82,92,101,102,115,138,157,213,237,240,258,262,310,436,439,442,458,464,474
Mandia, K (2003)	Sarbanes	0	
Mandia, K (2003)	Electronic crime	18	4,6,7,9,14,24,53,54,57,69,72,77,82,100,172,174,187,198
Mandia, K (2003)	Fraud	3	7,12,452
Mandia, K (2003)	Records	9	27,87,175,200,212,295,316,340,345
Mandia, K (2003)	Information security	3	17,64,72
Mandia, K (2003)	Compliance	3	28,174,212
Mandia, K (2003)	Record(s) and Record keeping	1	303
Mandia, K (2003)	Evidence	39	28,86,87,146,152,173,174,197,198,199,200,201,202,203,204,205,207,208,210,211,212,213,244,292,360,446,468
Marcella, A (2008)	Forensics	31	4,5,7,8,13,28,29,31,42,44,45,47,64,67,68,156,169,183,184,191,196,231,241,267,280,297,311,332,387
Marcella, A (2008)	Sarbanes	10	3,8,10,15,26,66,311,318,496
Marcella, A (2008)	Electronic crime	29	12,14,20,21,43,179,196,240,286,299,301,303,304,306,307,309,310,344,345,352,369,370,389,443,444
Marcella, A (2008)	Fraud	24	2,3,4,7,8,19,20,21,22,25,112,234,240,268,277,298,299,300,301,303,309,317,484
Marcella, A (2008)	Records	37	3,10,15,16,45,64,146,158,160,171,175,181,182,199,261,302,311,312,318,325,327,387,415,440,443,444,449,463,464,469
Marcella, A (2008)	Information security	15	2,14,15,25,35,55,57,144,161,197,295,322,353,420,491

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt
Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt
Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt
Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt
Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt
Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt
Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt
Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt
Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt
Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt
Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt
Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt
Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt
Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt
Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt
Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt

Marcella, A (2008)	Compliance	25	3,8,14,15,18,23,39,44,195,239,260,261,284,293,311, 314,318,322,325,326,327,328,477
Marcella, A (2008)	Record(s) and Record keeping	2	311,463
Marcella, A (2008)	Evidence	52	4,5,6,11,12,13,43,44,49,185,199,203,204,210,217,21 8,221,222,270,273,278,280,286,287,288,298,303,445 ,465,468
Muller, G (2006)	Forensics	0	
Muller, G (2006)	Sarbanes	5	12,13,18
Muller, G (2006)	Electronic crime	0	
Muller, G (2006)	Fraud	0	
Muller, G (2006)	Records	1	13
Muller, G (2006)	Information security	1	10
Muller, G (2006)	Compliance	0	
Muller, G (2006)	Record(s) and Record keeping	0	
Muller, G (2006)	Evidence	0	
Nelson, B (2006)	Forensics	53	1-8,14,21,22,23,28,29,33,34,39,40,49,51,57,59,98,133, 134,138,139,140,141,145,146,148,150-155,157,169-173,183,194,203,207,315,318
Nelson, B (2006)	Sarbanes	0	
Nelson, B (2006)	Electronic crime	3	23,58,137
Nelson, B (2006)	Fraud	1	137
Nelson, B (2006)	Records	4	211,212,440

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt

Nelson, B (2006)	Information security	0	
Nelson, B (2006)	Compliance	0	
Nelson, B (2006)	Record(s) and Record keeping	0	
Nelson, B (2006)	Evidence	37	3,33,34,35,36,37,38,39,46,47,48,49,50,51,52,53,54,55,56,57,58,59,135,165,209-222,229,231,247-253,467
Nolan, R (2005)	Forensics	42	19,21,22,23,24,29,44,51, 64,65,99,103, 177,179, 207
Nolan, R (2005)	Sarbanes	1	23
Nolan, R (2005)	Electronic crime	17	21,23,24,25,28,35,42,43,65,86,99,182
Nolan, R (2005)	Fraud	2	35,37
Nolan, R (2005)	Records	43	30,36,37,39,41,42,43,44,45,46,49,50,54,61,187,191
Nolan, R (2005)	Information security	7	1.71042E+13
Nolan, R (2005)	Compliance	5	23,34,41,42
Nolan, R (2005)	Record(s) and Record keeping	0	
Nolan, R (2005)	Evidence	78	21,22,23,24,26,28,29,30,43,44,45,46,48,64,74,79,86,92,101,106,107,109,179,182,183,187,188,189,
Rantala, R. (2008).	Forensics	0	
Rantala, R. (2008).	Sarbanes	1	9
Rantala, R. (2008).	Electronic crime	30	1,2,3,4,5,6,7,8,9
Rantala, R. (2008).	Fraud	12	1,2,3,4,5,6,7
Rantala, R. (2008).	Records	1	10
Rantala, R. (2008).	Information security	1	11
Rantala, R. (2008).	Compliance	0	
Rantala, R.	Record(s)	0	

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt

(2008).	and Record keeping		
Rantala, R.	Evidence	0	
Richardson, S. (2005).	Forensics	38	1,2,3,4,5
Richardson, S. (2005).	Sarbanes	9	1,2,4
Richardson, S. (2005).	Electronic crime	1	2
Richardson, S. (2005).	Fraud	6	1,2
Richardson, S. (2005).	Records	4	2,3,7
Richardson, S. (2005).	Information security	9	1,2,4,5,7
Richardson, S. (2005).	Compliance	24	1,2,3,4,5
Richardson, S. (2005).	Record(s) and Record keeping	0	
Richardson, S. (2005).	Evidence	1	5
Sarbanes-Oxley Act (2002)	Forensics	0	
Sarbanes-Oxley Act (2002)	Sarbanes	16	745,749,750,766,767,768,771,774,785,786,787,788
Sarbanes-Oxley Act (2002)	Electronic crime	2	804
Sarbanes-Oxley Act (2002)	Fraud	9	777,778,794,796,799,800,801,802,803,804,805,807,808,809
Sarbanes-Oxley Act (2002)	Records	11	756,758,760,771,780,801
Sarbanes-Oxley Act (2002)	Information security	0	
Sarbanes-Oxley Act (2002)	Compliance	19	747,751,754,756,757,767,768,776,778,784,790,791,794

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt

Sarbanes-Oxley Act (2002)	Record(s) and Record keeping	1	761
Sarbanes-Oxley Act (2002)	Evidence	8	784,802,809
Small, M. (2009).	Forensics	0	
Small, M. (2009).	Sarbanes	0	
Small, M. (2009).	Electronic crime	0	
Small, M. (2009).	Fraud	0	
Small, M. (2009).	Records	0	
Small, M. (2009).	Information security	0	
Small, M. (2009).	Compliance	0	
Small, M. (2009).	Record(s) and Record keeping	0	
Small, M. (2009).	Evidence	0	
Steel, C. (2006).	Forensics	26	1,2,3,4,5,6,7,8,16,31,34,45,54,58,96,138,169,171,220,259,290,294,299,309,327,331
Steel, C. (2006).	Sarbanes	2	28,29
Steel, C. (2006).	Electronic crime	27	1,6,8,9,11,12,13,14,17,18,20,21,22,23,25,29,36,168,284,364,366,367,370,372,374,377,378
Steel, C. (2006).	Fraud	4	12,138,207,327,
Steel, C. (2006).	Records	16	18,22,26,64,125,138,188,277,278,279,280,281,283,301,302,355
Steel, C. (2006).	Information security	2	6,28
Steel, C. (2006).	Compliance	1	75
Steel, C. (2006).	Record(s) and Record keeping	0	2,7,11,12,13,14,19,20,21,22,25,26,27,28,29,169,170,171,173,174,177,193,200,206,207,222,249,339
Steel, C.	Evidence		

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt

(2006).			
Vacca, J. (2005).	Forensics	28	1,3,4,6,8,9,10,17,21,29,35,36,57,75,83,162,280,297,386,665,684,699,705,709,713,717,718
Vacca, J. (2005).	Sarbanes	1	702
Vacca, J. (2005).	Electronic crime	26	4,5,6,12,35,37,141,153,154,155,156,182,229,230,238,278,287,288,358,471,674,681,682,699,700,750
Vacca, J. (2005).	Fraud	31	5,8,12,16,17,18,20,25,26,31,57,91,95,108,131,136,141,154,185,278,529,607,609,613,647,699,702,717,736,739
Vacca, J. (2005).	Records	30	10,16,58,64,70,89,102,150,168,206,218,219,277,283,317,319,320,321,457,470,553,570,576,605,614,675,683,694,719,817
Vacca, J. (2005).	Information security	23	132, 136,166,167,173,174,267,362,364,365,377,440,475,476,487,586,636,711,726,755,776,778,805
Vacca, J. (2005).	Compliance	6	97,253,329,622,729,732
Vacca, J. (2005).	Record(s) and Record keeping	5	8,18,20,31,277
Vacca, J. (2005).	Evidence	41	6,17,18,24,37,58,74,163,164,177,182,217,218,219,220,223,224,229,235,236,239,240,247,249,254,277,278,304,320,321
Volonino, L. (2003).	Forensics	14	3,7,8,9,10
Volonino, L. (2003).	Sarbanes	4	5,22
Volonino, L. (2003).	Electronic crime	3	8,10
Volonino, L. (2003).	Fraud	10	2,5,7,8,9,15
Volonino, L. (2003).	Records (e-records)	60	2,3,4,5,6,9,10,11,12,13,14,15,16,17,21,22
Volonino, L. (2003).	Information security	0	
Volonino, L.	Compliance	4	3,7,14,16

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt

(2003).			
Volonino, L. (2003).	Record(s) and Record keeping	0	
Volonino, L. (2003).	Evidence	49	2,3,4,6,7,8,9,10,11,12,13,15,17,20,21
Wolfe, H. (2007).	Sarbanes	0	
Wolfe, H. (2007).	Electronic crime	13	2,4,5,6
Wolfe, H. (2007).	Fraud	1	4
Wolfe, H. (2007).	Records	0	
Wolfe, H. (2007).	Information security	0	
Wolfe, H. (2007).	Compliance	0	
Wolfe, H. (2007).	Record(s) and Record keeping	0	
Wolfe, H. (2007).	Evidence	38	1,2,3,5,6,7

Linda Ettinger 6/5/09 8:40 AM
Formatted: Font:12 pt