# Understanding & Detecting Business Fraud: Accounting & Legal Issues

## Table of Contents


| Section | Subject |
|---|---|
| 1 | Detecting Financial Statement Fraud: Proposed SAS 82 Revisions |
| 2 | Fraud Risk Factor Examples |
| 3a | Advanced Data Recovery Outline |
| 3b | Advanced Data Recovery with Forensic Applications |
| 4 | The Auditor as Financial Policeman |
| 5 | Principles of Fraud Detection |
| 6 | Criminal Issues Facing Auditors and Accountants |
| 7 | Appointments as Special Master & Receiverships |

# Understanding & Controlling Business Fraud: Accounting & Legal Issues
# August 21, 2002

## Faculty Information

**J. Michael Inzina**, **CPA, CGFM**, is a partner in the St. Charles Parish (Louisiana) office of Stagni & Company, LLC, where his practice is concentrated in governments and nonprofit organizations. He also consults on audit efficiency. Mike is active with the AICPA, Louisiana Society of CPAs, the GFOA of Louisiana, and the Association of Certified Fraud Examiners. He is a member of the AICPA Auditing Standards Board and has served on several other AICPA committees and subcommittees. Mike's outstanding teaching ability has been recognized by the AICPA and the Louisiana, South Carolina and West Virginia Societies of CPAs. Mike has participated in several ACPEN programs in the governmental and not-for profit areas.

**Susan L. Menelaides, CPA**, is a Partner in the Quality Assurance group for Altschuler, Melvoin and Glasser LLP. She is responsible for overseeing the firm's quality control functions over all accounting and auditing services. Her responsibilities include establishing and maintaining the firm's policies and procedures for conducting audit and accounting engagements, serving as a consultant to clients and firm personnel on technical matters, developing the firm's technical training curriculum, and ensuring that audited financial statements and other reports issued by the firm comply with professional standards. Susan has been a member of the AICPA's Fraud 2000 Task Force since its inception in September 2000. The Task Force's recommended changes to SAS 82 are expected to be approved by the AICPA's Auditing Standards Board in July 2002. Before joining AM&G, Menelaides served as Director of the Technical Information Division for the American Institute of Certified Public Accountants (AICPA), where she managed a staff that answered more than 50,000 questions annually from CPAs across the country on a variety of accounting and auditing issues. Menelaides and her staff also wrote and edited more than 50 technical publications for CPAs. Prior to joining the AICPA, she spent three years with a publishing company in Texas, and a total of 10 years with two of the Big Five accounting firms in Houston and Las Vegas, working with a broad spectrum of clients including financial institutions, hotel/casinos, real estate developers, oil field service companies, and nonprofit organizations. Menelaides has a Bachelor of Business Administration in accounting from Texas Tech University. She is an AICPA member and the Illinois Society of CPAs, and serves as director and treasurer for the Chicago Finance Exchange and Urban Gateways.

**Charles W. Blau, JD,** is a partner in the law firm of Meadows, Owens, Collier, Reed, Cousins & Blau, L.L.P., in Dallas, Texas. He focuses his practice on the representation of individuals and entities that are accused of white collar crimes. Mr. Blau assists companies in discrete internal investigations both before and during governmental inquiries. He also aids corporations in fashioning, enacting and administering compliance and ethics programs. He regularly advises clients how to prevent and detect criminal, civil and administrative problems, often in conjunction with independent accountants and investigators. His practice concentration and experience includes criminal law and litigation: Tax Fraud, Criminal Anti-Trust and Securities Fraud, Defense Procurement Fraud, Environmental Crimes, Health Care Fraud, Bank Fraud and Money Laundering Crimes. Mr. Blau was an Assistant United States Attorney for the Southern District of Indiana in 1976 and held various federal prosecutorial positions through 1987, including Associate Deputy Attorney General of the United States. He is a prolific author and speaker. He is an active member of the ABA White Collar Crime Subcommittee and served as a co-chair of the Southwest Regional Committee of the organization. He is member of the Florida, Indiana and Texas bar associations as well as many other professional organizations. He received his undergraduate degree from Indiana University, his law degree from the University of Louisville and his L.L.M. in taxation from Georgetown University.

**Phillip Umphres, JD**, is an Assistant United States Attorney in Dallas, Texas. He is a native of Amarillo, Texas, a 1977 graduate of the University of Texas School of Business Administration (where he majored in Accounting, receiving a BBA degree with Highest Honors) and is a 1980 graduate of Harvard Law School. Following law school, Mr. Umphres served 4 years as a criminal trial lawyer in the U.S. Army Judge Advocate General's Corps. After leaving the Army, Mr. Umphres worked as a civil trial lawyer in the Dallas office of Akin, Gump, Strauss, Hauer and Feld, where he was a partner engaged primarily in general business litigation. Some of the cases he worked on involved allegations of malpractice by auditors, one resulting in a multimillion dollar settlement by a then "Big 8" accounting firm. Since 1991 he has been an Assistant United States Attorney in Dallas, where he specializes in prosecuting white collar frauds. He is currently the Health Care Fraud Coordinator for the Northern District of Texas. Many of the cases he works on involve allegations of fraudulent financial statements. He has handled the investigation of several accountants alleged to have assisted in fraudulent schemes by either preparing or failing to correct false financial statements; a CPA implicated in one of the investigation was convicted of fraud and sent to federal prison.

**Thomas J Kapurch** is a former Intelligence Officer, US Navy and Defense Intelligence Agency, with more than 15 years experience in information systems, intelligence collections, analysis, technical information systems, geo-political intelligence and military investigations. His industry experience includes over ten years in business and information systems management for GTE, Nextel, NEC America, TXU, Informatica Software Company with eleven years experience

developing business and operations plans, as internal and external information systems consultant to telecommunications, utilities and financial companies. Mr. Kapurch also worked as an engineer with Texas Instruments on computer based aerospace products with OEMs and major subcontractors Bell Textron, McDonnell-Douglas, Boeing and Lockheed. While at TI Kapurch also managed all phases of electronics systems and components manufacture and enterprise wide information systems for manufacturing and shipping. He is currently Vice-President of Data Recovery Services Inc. in Dallas, Texas, responsible for designing and presenting technology seminars for litigation support and government services.

**Dale V. Hogue,** is a Special Agent with the Federal Bureau of Investigation (F.B.I.), at its Dallas field office. He has 26 years of investigative and law enforcement experience, much of it focusing on fraud in businesses of all types. He has also been a Technical Trained Special Agent responsible for various types of sophisticated investigative techniques and tools as well as a member of a Foreign Counter-Intelligence Squad. Prior to joining the FBI, Dale was an accountant at an accounting firm in Oklahoma City. He holds a Bachelor of Business Administration-Accounting from the University of Oklahoma. Dale's broad range of experience with the FBI includes numerous successful white-collar crime, public corruption and other criminal investigations. He was the case agent responsible for a two billion dollar bank failure investigation that resulted in the conviction of 25 individuals. He recently received a Certificate of Commendation in a major health care fraud case. Dale has been an instructor at the FBI Academy and for the International Training Unit of the FBI in which white-collar crime investigation seminars were presented in Russia and various other countries in eastern Europe and Asia.

**RALPH S. JANVEY,JD,** is a partner in the Dallas, Texas law firm of Krage & Janvey, L.L.P. His practice involves advising individuals and entities (including Issuers, Broker-Dealers and Investment Advisors) on organizational structuring, financing, and federal and state administrative compliance issues. He is the author of Regulation of the Securities and Commodities Markets published by Warren, Gorham & Lamont, Inc.; Accountant's Liability Manual published by Clark Boardman Callaghan; and SEC Accounting and Reporting published by the Texas Society of Certified Public Accountants. Mr. Janvey is also an NASD arbitrator, court appointed receiver in SEC fraud litigation, an adjunct professor of law at Southern Methodist University and a member of the Boards of Editors of the Journal of Corporate Confidentiality and the Securities Regulation Law Journal.

# Section 1

# Detecting Financial Statement Fraud: Proposed SAS 82 Revisions

Susan Menelaides, CPA
Altschuler, Melvoin & Glasser, LLP
Chicago, Illinois

# Detecting Financial Statement Fraud: Proposed SAS 82 Revisions

## Background

- SAS 82 issued in 1997 to:
  - Enhance auditor performance in detecting material misstatements due to fraud
  - Provide auditors with additional operational guidance

- When issued, AICPA Auditing Standards Board committed to revisiting effectiveness after implementation
  - Led to ASB-sponsored research on SAS 82 in 1999 and to formation of current task force

## Task Force Objectives

- Consider need for revisions based on:
  - Results of academic research
  - Recommendations of the Public Oversight Board's Panel on Audit Effectiveness regarding earnings management and fraud
  - Information from various stakeholders

- Coordinate with international standards setters

## Current Status

- Exposure period ended - May 31, 2002

- Expected approval by Auditing Standards Board – August 2002

- Target issuance of new SAS - Late 2002

  - Effective for audits of financial statements beginning after December 15, 2002

- Plans to develop implementation guidance and training

## AICPA Fraud 2000 Task Force

- Task Force members and observers representing -
  - CPA firms - all sizes
  - forensic expertise
  - academia
  - internal audit
  - technology expertise
  - international perspectives
  - legal expertise

## Task Force's Approach

- Reviewed results of AICPA-sponsored academic research
- Reviewed input from AAA literature search
- Studied Panel on Audit Effectiveness' recommendations on earnings management and fraud
- Interviewed various stakeholders – auditors from firms of all sizes, forensic experts, internal auditors, academics, technology experts, etc.

## SAS 82 Academic Research

- 4 sponsored research projects examined
  - Risk factors included in SAS 82 and other indicators of fraud
  - Auditors' ability to identify fraud risk
  - How auditors responded to fraud risk factors
- AICPA Monograph - Focus on Deficiencies
  - *Fraud Related SEC Enforcement Actions Against Auditors: 1987-1997*

## Key Messages from Research

- SAS 82 has heightened auditors' sensitivity to identification of fraud risk
- Auditors respond to fraud risk by
  - changing ***staffing*** and increasing ***extent*** of testing;

– but the ***nature*** of tests changed less often

- Some risk factors are more important, but insufficient evidence to allow weighting

## Key Messages from Interviews with Stakeholders

- Inquiry is an important audit technique
  – and enhanced interviewing skills are needed

- List of fraud risk factors is not discriminating

- Linking of fraud risk factors identified with auditor's response has been difficult

- Greater emphasis on skepticism is necessary

- Differences exist between public and private entities

## Auditor's Responsibility for Fraud

- SAS 82 says an auditor has a responsibility *"to plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement, whether caused by error or fraud."*

- This basic responsibility is ***unchanged***

# Proposed SAS – Overview

- Description of characteristics of fraud
- Discussion among audit team members
- Information gathering
- Assessing risks of fraud
- Evaluating management's responses
- Developing auditor's response
- Evaluating audit results
- Communication requirements
- Documentation requirements

# Proposed Revisions

- Description of characteristics of fraud
  - 2 types -
    - fraudulent financial reporting
    - misappropriation of assets
  - Three conditions always present when fraud occurs – incentives/pressure, opportunity, and attitude/rationalization that allows one to commit fraud
    - all three conditions may not be observable to the auditor
  - Often concealed - collusion or falsified documentation
  - Management's ability to override controls always present to some degree
- Required discussions among engagement team members
  - Brainstorming - "Where could fraud occur and how could it happen?"
  - Sharing of information and insights of more experienced engagement team members
  - Emphasis on professional skepticism - *"An attitude that includes a questioning mind and a critical assessment of audit evidence"*
  - The form of this discussion and who participates is left to the lead audit partner's judgment
- Expanded information gathering process
  - Expand inquiries of management and others
    - Obtain their views about the risk of fraud
    - Understand programs and controls to mitigate risks
    - Determine if management has knowledge of fraud
    - Include audit committee, internal audit, operational management, etc. in these inquiries

- Consider presence of risk factors (fraud risk factors now presented in an Appendix as example fraud risk factors)

- Review planning analytics

- Consider other information -- i.e., information from client acceptance process, interim reviews of public company financials, assertions involving high inherent risk (such as revenues when revenue recognition policy is highly subjective)

• SAS 82 Fraud Risk Factors – now presented as examples to consider in an Appendix to the SAS.

  - Fraudulent Financial Reporting
    · Management characteristics and influence over the control environment
    · Industry conditions
    · Operating characteristics and financial stability

  - Misappropriation of Assets
    · Susceptibility of assets to misappropriation
    · Controls

# Examples of Fraud Risk Factors for Fraudulent Financial Reporting

- **Incentives/Pressures**
  - Excessive pressure on management to meet earnings expectations due to:
    - **Profitability expectations of investors, investment analysts, etc.**
    - **Need to obtain additional debt or equity financing to stay competitive**
  - Management or the board's personal net worth is threatened by the entity's financial performance due to:
    - **Personal guarantees of the debts of the entity that are significant to their personal net worth**
    - **Significant portions of compensation being contingent upon achieving aggressive targets**
- **Opportunities**
  - Inadequate monitoring of internal controls
  - Significant accounting estimates involving subjective judgments
  - Significant related party transactions not in the ordinary course of business or with related entities not audited or audited by another firm
  - Significant, unusual or highly complex transactions, especially those close to year end that pose difficult substance over form questions
- **Attitudes/Rationalization**
  - Management attempts to justify marginal or inappropriate accounting practices
  - Management is interested in using inappropriate means to minimize reported earnings to avoid taxes

# Proposed Fraud Risk Factors
# Misappropriation of Assets

- **Incentives/Pressures**
  - Adverse relationships between entity and employees
  - Personal financial obligations that create pressure on management or employees with access to cash or other assets to misappropriate those assets
- **Opportunities**
  - High value, small size, high demand inventory
  - Inadequate internal control over assets, such as
    - **Inadequate segregation of duties**
    - **Inadequate safeguards over cash, investments, inventory, or fixed assets**
    - **Inadequate access controls over automated records**
- **Attitudes/Rationalization**
  - Disregard for monitoring and controls
  - Failure to correct known internal control deficiencies
  - Changes in behavior or lifestyle or behavior indicating displeasure or dissatisfaction with the company
- Identifying and assessing fraud risks after taking into account programs and controls to prevent, deter and detect fraud
  - Information gathered is used to identify fraud risks that may result in a material misstatement of the financial statements

- For each risk identified, evaluate management's programs and controls to prevent, deter and detect fraud
- Separate initiative addressing Anti-Fraud Programs & Controls -- e.g.
  - Creating a **culture** of honesty and high ethics
  - **Evaluating** processes and controls aimed at mitigating the risks of fraud
  - Developing an effective **oversight** process
- Revenue recognition as a fraud risk
  - "Ordinarily" a risk that should be identified
  - Expanded guidance regarding auditor response to the risk
- Management override of controls as a fraud risk

• Linking the fraud risks to the auditor's response

- Overall responses
  - Professional skepticism -- e.g., design procedures to obtain more reliable evidence and additional corroboration of management's explanations
  - Assignment of personnel and supervision – e.g., assign persons with specialized skill or knowledge or more experienced persons
  - Review of accounting principles – e.g., consider whether accounting principles selected indicate, on a collective basis, a bias by management to misstate the financials.
  - Predictability of auditing procedures – e.g., test accounts not normally tested, change timing of testing, and perform surprise counts.
- Responses focused on specific accounts or classes of transactions, with expanded examples

    - Guidance on changing the nature, timing and extent of auditing procedures – e.g., more evidential matter from external sources, physical inspection or observation of certain assets; interim versus year-end testing; increased sample sizes and more detailed analytical procedures
    - Expanded examples of how to apply to e.g., revenue recognition, inventory quantities, restructuring reserves
  - Responses to address management override
    - Examining journal entries
    - Reviewing accounting estimates for biases
    - Evaluating business rationale for significant unusual transactions
  - Applicability –
    - Generally presumed to be appropriate for all audits
    - Required for audits of public companies
- Procedures to address risk of management override is not always required, such as for:
  - A nonpublic or not-for-profit with little "incentive/pressure" to achieve specified results
  - An employee benefit plan with little "incentive/pressure" to misstate financial results
- Expanded guidance on evaluating results at end of audit
  - Conditions indicative of fraud
  - Year-end analytical relationships
  - Implications of adjustments
- Expanded documentation requirements

## Overall Goal of Proposed Revisions

- Improve the likelihood that auditors will detect material misstatements due to fraud
- Create an impact that results in a substantial change in auditor performance

## 49 Comment Letters to ED Received

- Comment letters generally supportive – no single issue was focal point of comments
- Larger firms in fact are adopting early
- Medium and small firms are supportive; some concerns about added cost when fraud risk is relatively low
- Significant observations and issues raised:
  - Risk factors - strong support for categorizing risk factors along the three conditions present when fraud occurs – incentives/pressures, opportunity, attitudes/rationalization
  - Communication among engagement team - requests for elaboration on the nature and purpose of the communication. Many suggested a similar communication be held at the conclusion of the audit.
  - Revenue recognition as an "assumed" fraud risk – ED states auditors will "ordinarily" consider revenue recognition as a fraud risk. Commentators indicated that this should not be presumed for many private companies
  - Entity Programs and Controls – request for additional discussion of what these programs and controls might include, and for discussion of management's responsibility to prevent, deter, and detect fraud.

– Mandatory procedures to address risk of management override of controls. Commentators were mixed – some indicated the requirement is too stringent for nonpublic companies; others indicated it should be applied to all entities

– Broad support on for emphasis on professional skepticism; POB urged expanding discussion – auditors should be alert for the possibility of fraud throughout the audit

## Future Research Needs

- More intense study of common threads of failed audits
- Continued assessment of comparative performance pre and post SAS 82 and ED
    - Fraud risk identification
    - Linkage of risks with auditor response
- Relevance and weighting of risk factors
- Environmental variables affecting professional skepticism
- The validation/questioning of basic ED premises -- e.g:
    - The extent engagement team discussions do, in fact, reinforce professional skepticism
    - Which analytical relationships best identify fraud
    - The ED's approach to management override
    - Whether documentation requirements affect auditor performance

# Section 2

# Fraud Risk Factor Examples

J. Michael Inzina, CPA, CGFM
Stagni & Co., LLC
St. Rose, Louisiana

**FRAUD RISK FACTOR EXAMPLES**

**Fraudulent Financial Reporting**

## Incentives/pressures

- Financial stability or profitability threatened by economic, industry or entity operating conditions:
    - High degree of competition or saturation, accompanied by declining margins
    - High vulnerability to rapid changes, e.g., technology product obsolescence, interest rates
    - Significant declines in customer demand and increasing business failures in the industry or overall economy
    - Operating losses making the threat of bankruptcy, foreclosure or hostile takeover imminent
    - Recurring negative cash flows from operations or the inability to generate operating cash flows while reporting earnings and earnings growth
    - Rapid growth or unusual profitability when compared to other companies in the same industry
    - New accounting, statutory or regulatory requirements
- Excessive pressure exists to meet the requirements or expectations of third parties:
    - Expectations of analysts, institutional investors, significant creditors or other external parties, including those that are overly aggressive or unrealistic
    - Need to obtain additional debt or equity financing to stay competitive (including financing of major research and development or capital assets)
    - Marginal ability to meet debt repayment or other debt covenant requirements
    - Perceived or real adverse effects of reporting poor results on significant pending transactions (such as business combinations or contract awards)

- Management or board's personal net worth is threatened by the entity's financial performance arising from:
    - Heavy concentrations of personal net worth in the entity
    - Significant portions of compensation (such as bonuses, stock options) being contingent upon achieving aggressive targets for stock price, operating results, financial position or cash flow
    - Personal guarantees of debt of the entity that are significant to management or board's net worth
- Excessive pressure on management or operating personnel to meet financial targets established by the board or management, including sales and profitability goals.

## Opportunities

- The industry or entity provides opportunities to engage in fraudulent financial reporting from:
    - Significant related party transactions not in the ordinary course of business or with related entities not audited or audited by another firm
    - Assets, liabilities, revenue or expenses based on significant estimates that involve subjective judgments or uncertainties that are difficult to corroborate
    - Significant, unusual or highly complex transactions, especially those at or near year-end, that pose difficult "substance over form" questions
    - Significant operations located or conducted across international borders in jurisdictions where differing business environments and cultures exist
    - Significant bank accounts or subsidiary operations in tax-haven locations for which there appears to be no sound business reasons
- Ineffective monitoring of management resulting from:
    - Domination of management by a single person or small group (in a non-owner managed business) without compensating controls
    - Ineffective board of directors or audit committee oversight of the financial reporting process and internal controls
- Complex or unstable organizational structure evidenced by:
    - Difficulty in determining the organization or individuals who control the entity
    - Overly complex organizational structure involving unusual legal entities or managerial lines of authority
    - High turnover of senior management, counsel or members of the board
- Internal controls are deficient as a result of:
    - Inadequate monitoring of controls, including automated controls and controls over interim financial reporting (where external reporting is required)

- High turnover rates or employment of ineffective accounting, internal audit or IT staff

- Ineffective accounting and information systems, including situations involving reportable conditions

## Attitudes/rationalizations

[Clearly it may not be possible for the auditor to observe risk factors related to attitudes and rationalizations by board members, management or employees. However, the auditor should be alert to the existence of these and similar risk factors that do manifest themselves.]

- Ineffective communication and support of the entity's values and ethical standards, or the communication of inappropriate values and ethical standards

- Non-financial managers' participation in the selection of accounting principles, particularly those related to estimates in the financial statements

- Known history of securities violations, or violations of other laws and regulations, or claims against the entity, senior management or board members alleging fraud or violations of laws or regulations

- Excessive interest by management in increasing or maintaining the stock price or earnings trend

- A practice by management of committing to analysts, creditors or other third parties to achieve aggressive or unrealistic forecasts

- Management's failure to correct known reportable conditions timely

- An interest by management in using inappropriate means to minimize reported earnings for tax purposes

- Recurring attempts by management to justify marginal or inappropriate accounting practices based on materiality

- A strained relationship between the management and the current or prior auditor, such as:

    - Frequent disputes on accounting, auditing or reporting matters

    - Unreasonable demands on the auditor, including time demands for completion of the audit or release of the report

- Formal or informal restrictions on the auditor that inappropriately limit access to personnel or information or the ability to communicate effectively with the board or audit committee

- Domineering management behavior in dealing with the auditor, especially that involving attempts to influence the scope of the auditor's work or the selection or continuance of audit personnel assigned to the engagement

## Misappropriation of Assets

### Incentives/pressures

- Personal financial obligations may create pressure on management or employees with access to cash or other assets susceptible to theft to misappropriate those assets

- Adverse relationships between the entity and employees with access to cash or assets susceptible to theft may motivate those persons to misappropriate those assets, such as:

    - Known or anticipated layoffs

    - Promotions, compensation or other rewards inconsistent with expectations

### Opportunities

- Characteristics or circumstances may increase the susceptibility of assets to misappropriation, such as:

    - Large amounts of cash on hand or processed

    - Inventory items that are small, high value or in high demand

    - Easily convertible assets, such as bearer bonds, diamonds or computer chips

    - Fixed assets that are small in size, marketable or that lack observable identification of ownership

- Inadequate controls over assets may increase the susceptibility to misappropriation, such as:

    - Inadequate segregation of duties or independent checks

- Inadequate management oversight of employees responsible for assets
- Inadequate job applicant screening of employees with access to assets susceptible
- Inadequate record keeping of assets susceptible to misappropriation
- Inadequate system of authorization and approval of transactions
- Inadequate physical safeguards over cash, investments, inventory or fixed assets
- Lack of timely and appropriate documentation of transactions, such as credits for merchandise returns
- Lack of mandatory vacations for key employees
- Inadequate management understanding of information technology, enabling IT employees to perpetrate a misappropriation
- Inadequate access controls over automated records

## Attitudes/rationalizations

[See previous comment under fraudulent financial reporting.]

- Disregard for the need for monitoring or reducing risks related to misappropriation of assets
- Disregard for internal control over misappropriation of assets by overriding existing controls or by failing to correct known internal control deficiencies
- Behavior indicating displeasure or dissatisfaction with the entity or its treatment of the employee
- Changes in behavior or lifestyle that could indicate that assets have been misappropriated

# FRAUD PREVENTION
## Steps Management Should Take in Preventing the Occurrence of Fraud

- **Control the mail** – In small businesses, owner/management should either personally pick up the mail, or have the mail picked up by an employee who has no responsibilities related to the handling or recording of deposits, accounts receivable records or revenues. All remittances from customers should be directed to a post office box. Limiting access to the company's mail is essential in preventing the unauthorized negotiation of cash receipts.

- **Control the bank statements** – Similarly, the owner/management should personally pick up the company's bank statements directly from the bank, or have them picked up by an employee who has no related responsibilities. Owner/management should review the contents of the statements before they are reconciled. Specific items that management should be alert to include:
    - Missing checks
    - Checks issued out of sequence
    - Unknown payees
    - Checks that appear to have been altered
    - Checks not signed by authorized signatories
    - Other unusual items

- **Control the accounts receivable** – Owner/management should limit access to accounts receivable records, and in particular, the ability to issue credit memoranda, discounts and refunds. Accounts receivable detail ledgers should be balanced with the control account at regular intervals and any differences should be investigated promptly. Only owner/management should be authorized to charge off accounts deemed uncollectible. Any discrepancies reported by customers should be investigated promptly. Aged accounts should be reviewed monthly and past due accounts investigated.

- **Control the inventory** – Owner/management should carefully monitor gross profit, and investigate any unexpected variances. Access to inventories should be limited as much as possible, and the use of surveillance equipment may deter inventory theft. If a perpetual inventory is used, periodic counts should be performed at regular intervals for comparison with the perpetual records.

- **Control the accounts payable** – Establish and monitor approved vendor lists. Owner/management should periodically review the list of approved vendors, being alert to:
    - Unknown vendors
    - Vendors with names similar to other known vendors
    - Vendors with no physical address or telephone number
    - Vendors whose addresses match employee addresses

- **Limit the number of authorized check signers** – If possible, only the owner/manager should be authorized to sign checks. If not possible, consider requiring two signatures on checks, at least those over a specified amount. The use of facsimile signatures should be avoided if at all possible. Never sign checks in blank. Review supporting documentation when checks are signed and investigate any discrepancies.

- **Account for sequences** – Whether it is checks, invoices, credit memoranda, receiving reports, shipping documents, or other pre-numbered items, all sequences should be accounted for. Voided documents should be defaced to prevent unauthorized use and retained to complete sequences.

- **Control general journal entries** – Owner/management should either make or personally review and approve all general journal entries. Supporting documentation should be reviewed before approving general journal entries. In particular, the following items should be investigated:
    - Entries made to unrelated accounts
    - Entries made to receivables or revenues at or near the close of a period
    - Entries made by persons whose responsibilities are not consistent with the accounts being adjusted

- **Monitor exception reports** – Unprocessed transactions should be carefully examined for propriety. This includes revenues, expenses, purchasing and payroll transactions.

- **Establish a budget** – Owner/management should establish an operating budget and monitor actual results monthly. Any significant variances should be investigated.

- **Establish reasonable performance targets** – Setting incentive compensation arrangements at unrealistic performance levels may encourage misstatement of financial results.

- **Be alert to changes in employee attitudes, behavior and lifestyles** – Because of day-to-day contact, management is in the best position to observe the unusual – attitudes that are hostile or defensive toward management or the company in general, changes in behavior that are inconsistent with employees' normal disposition or lifestyles that are not reasonable based on the employees' level of compensation. Matters that may be of particular concern include:
    - Indications of dissatisfaction with compensation, lack of promotion
    - Indications of gambling
    - Indications of drug use or excessive use of alcohol
    - Indications of financial distress
    - Indications of infidelity
    - Indications of serious illness
    - Indications of excessive nervousness

- Indications of severe stress

- **Perform background checks on all new employees** – Call former employers and educational institutions for verification of previous employment and education. Consider obtaining a credit report (if authorized by the candidate) before employment.

- **Require uninterrupted vacations for all employees and establish a schedule of rotation of employee responsibilities** – More than just good management, rotation of duties provides a strong disincentive to commit fraud, it provides an opportunity to discover fraud that has already occurred.

- **Obtain reasonable fidelity bond coverage** – If the unthinkable occurs, insurance coverage is the most likely means of recovery of amounts misappropriated. The amount of coverage should be reviewed periodically for adequacy.

# Section 3a

# Advanced Data Recovery Outline

Tom Kapurch
Data Recovery Services, Inc
Dallas, Texas

# Advanced Data Recovery and the Legal Profession
# A Continuing Education Course

**TX MCLE Course # 000030851**

**Presented by**

**Data Recovery Services, Inc**

**Dallas, TX**

# Advanced Data Recovery and the Legal Profession
# A Continuing Education Course

**TX MCLE Course # 000030851**

## Outline

**Introduction** General relevance of data believed lost, damaged or destroyed.

I. Legal considerations in preparation for recovery
   - A. General Application
   - B. Evidentiary Application
     1. Protection and preservation of original evidence
     2. Imaging

II. Technical Background
   - A. How electronic data storage devices work
     1. Magnetic media
     2. CDs and CD ROMs
   - B. Symptoms, causes and types of data failure
     1. Mechanical failure
     2. Deliberate deletion
     3. Software corruption and viruses

III. Data Recovery
   - A. General Business Matters
   - B. Evidentiary
     1. Protection and Preservation of original data
        - a. Proper storage
        - b. Chain of custody
     2. Expert testimony of recovery technicians
   - C. Recovery
     1. Basic
     2. Advanced

IV. Case Studies

V. Other Considerations
   - A. Recovery from catastrophic physical damage
   - B. Storage, Duplication, Conversion of Outdated Tape Formats
   - C. Trends
   - D. Implications for legal and business
   - E. Advanced Data Recovery Services

VI. Summary

# Advanced Data Recovery and the Legal Profession
# A Continuing Education Course

**A Continuing Education Course**
**TX MCLE Course # 000030851**

## Introduction.

Regardless of specialty, when required an attorney's job may be defined by a single but critical function – gathering, analyzing and presenting evidence. Whether pertaining to civil or criminal law, the basic process is the same – collect pertinent data prepare it according to proper evidentiary rules and present it.

For the past twenty years, and especially with the recent proliferation of the Internet, digital technology has changed greatly. More and more digital data is created, recorded and stored on PCs as well as palm pilots, pagers and mobile phones. These devices are used universally, not only to improve productivity but in every aspect of our personal lives. Consequently, all of these devices are also commonly used to commit crimes and civil wrong doings.

**Figure 1. Typical workstation.**

Digital evidence can be critical to the outcome of legal cases, civil and criminal. Recovery of *digital evidence*, even if assumed to be lost, corrupted or destroyed, can affect legal judgments, and a new set of recovery parameters needs to be understood and applied.

**Figure 2. Open hard drive exposing storage platter.**

When legal or law enforcement investigators must rely on evidence obtained from computers to prove their cases, the method by which digital data *is recovered* can be critical to the outcome of the case.

This course is designed to address one area of ***digital data collection*** and provide an understanding of how data storage works, and how data that is lost, damaged or corrupted and how it can be recovered for use as legal evidence.

This course uses real world cases to provide a foundation with which attorneys might ask appropriate how's, what's and why's when attempting to collect digital evidence. Attorneys will become familiar with the general capabilities of advanced data recovery and the correct legal, physical and evidentiary rules.

## I. Legal considerations in preparation for recovery

**A. General Application.** Data recovery is a process to recover what appears to be lost or irretrievable from electronic media storage devices, BUT IN ALL LIKELIHOOD IS STILL THERE.

Many conventional computer repair services perform relatively simple procedures with off-the-shelf software recovery that essentially can reclaim simple deleted files or repair media sectors or partitions. Firms that advertise a forensics capability also use conventional software recovery procedures that may or may not be targeted to the specific needs of the case. Reliance on either of these levels of recovery alone may result in the potential to miss all of the accessible data that is available for use in a court of law.

It is likely that in 50% of all lost data cases much of the critical data needed to affect a legal outcome is never retrieved. Our experience suggests that most failures occur due to a general lack of understanding about data recovery, even among seasoned computer technologists.

**B. Evidentiary Application.** Hardware and software often fail or are physically damaged; files are routinely, deliberately and accidentally deleted. Many attorneys often conclude (or are counseled to assume) that a loss or corruption of, or damage to, data or storage media is permanent. This is often not the case.

> **"Since 1992 the number of computer crime cases sent to federal prosecutors has tripled, while the number of cases actually prosecuted has remained the same.**
>
> **Of the 419 cases referred to prosecutors, only 83 were prosecuted. The rest were dismissed due to lack of evidence."**
>
> ***Electronic Privacy Information Center (EPIC)***
> ***January 29, 2001***

If an attorney is not aware of some of the advanced data recovery techniques needed to further investigate whether or not files are still present (due to more sophisticated SW or HW tampering), important case data may never be discovered. If a technician performing a recovery is not aware of proper forensics or chain of custody procedures required by the court, no matter how successful the recovery, use of digital evidence may be inadmissible.

When the possibility that digital evidence may have a bearing on a case attorneys need to understand both the limits of the various levels of data recovery, and the methods need to protect and preserve original evidence.

> **Attorneys "need to understand enough about (digital) … technology to ask the right questions and enlist the assistance of the forensic computer experts where necessary. *Lawyers who choose to ignore these new opportunities could expose themselves to malpractice claims."***
>
> ***Alan Gahtan***
> ***Brown Raysman, Millstein, Felder & Steiner LLP***

**Imaging and custody chain.** Imaging is used to capture original digital data without changing or writing over it, and creating an exact duplicate of the original drive contents. Since the image is an exact replication of the original, data recovery efforts can be performed on the image and the original drive can be sealed and stored. Knowing how to

apply this element of recovery has implications for correct chain of custody. (This is discussed in more detail on page seven.)

## II. Technical Background

**A. How electronic data storage devices work.** Data is generally stored or written, and then accessed or read in one of two ways.

**Magnetic tapes, diskettes hard disk drives** (HDDs) use computer signals to 'rearrange' iron (Fe) oxide properties on coated plastic film.

**Figure 3. Common hard drive devices**

**Figure 4. "Floppy" disks.**

In each case, whether with a hard drive, floppy disk or magnetic tape, data storage is affected by passing an electromagnetic charge onto iron oxide coated plastic. (red lines, Figure 5.)

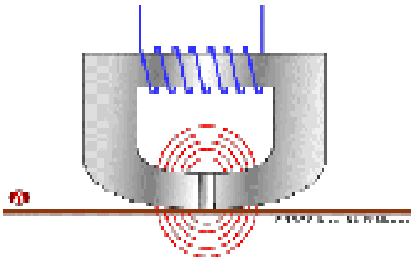
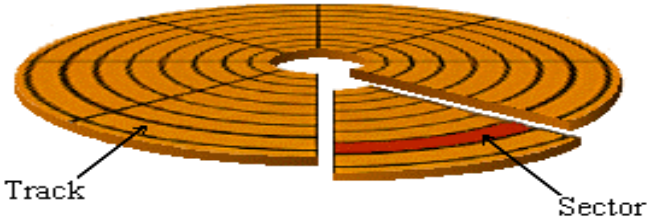


**Figure 5. Electromagnetic current passes over tape or platter.**

A hard drive or diskette platter resembles a vinyl record. It spins, records and accesses data with a device that rides above the disk, just as a record's music "groove" is read with a needle. [1]

Tracks and sectors on the platter physically divide and organize data. A set of instructions on one of the tracks tells the drive how to perform its mechanical functions, i.e. how fast to spin the platter and how to work the electronics




**CDs** Factory programmed plastic CDs, are aluminum-coated disks with impressed microscopic "bumps"; blank CDs uses dye coating instead of aluminum.

[1] The read/write device cannot touch the platter, as this is actually one cause of data failure or crash.

CDs and CD ROMs are molded pieces of clear plastic. On pre-recorded CDs the aluminum-coated plastic is impressed with microscopic "bumps" arranged on a single, continuous (similar to vinyl records), spiral track and layered with aluminum. Microscopic bumps are what the laser reads similar to the way electronically charged oxide is read by magnetic devices.

CD ROMs used for data backup use a dye coating rather than aluminum. As a CD is recorded, the CD "burner" laser heats spots on the dye causing the spots to darken. When reading or retrieving saved data, the laser thinks each "burnt spot" is a bump and reads the data in the same way it would a pre-recorded CD.

**B. Symptoms, causes and types of data failure** There are a variety of common symptoms that indicate data failure has occurred:

- a drive, diskette or tape device appears to be inaccessible,
- a system fails to boot showing a blue screen with unfamiliar instructions,
- an application fails to "open," run correctly, or accept data, or
- a mechanical component fails – failure of the drive to "spin" or clicking sounds.

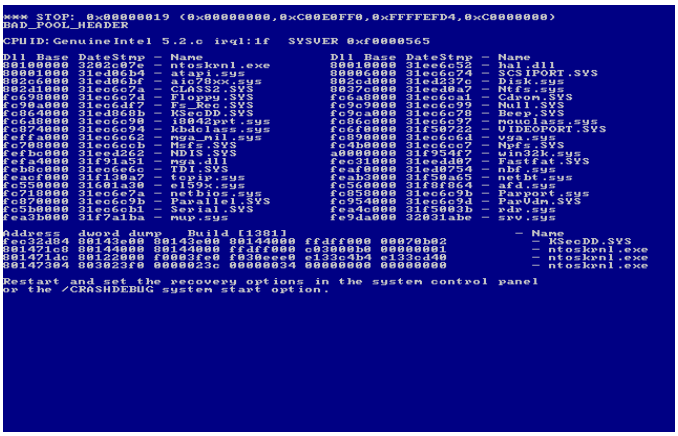



**Figure 6 The "Blue Screen of Death" – indication of serious data or sector damage.**

**Mechanical failure** appears to be the leading cause of data failure. This may occur due to accidents and catastrophic events – such as earthquakes, floods, fire, electrical failure and power surges. Age or abnormal wear (fairly new, well-built systems that sometimes just fail) are among other leading causes of failure.

**Software failure** can occur when there has been improper hardware or software handling or from viruses. This type of failure can occur either by deliberate intent to corrupt or through human error, such as with accidental reformatting or deletion of, or "writing over" of data files.

**Mechanical or software failure** A person intent on doing so, and with the proper knowledge, can induce mechanical or SW failure in order to hide evidence. The truly savvy

user can also replicate any of these symptoms, malfunctions or causes to mask their activities. Certainly arson and other physical misuse can be obvious; however, SW corruption, viruses, the improper loading or use of diagnostic or repair tools are not so obvious. Many times a user will claim files have been "mysteriously erased." It takes a technical specialist to distinguish cause from effect and know how to uncover evidence not readily available from a basic recovery. [2]

In order to affect a successful recovery a technician needs to know how to recognize if and how a system component has failed, or if the file that holds critical data is actually damaged. [3]

## III. Data Recovery

**A. General Business Matters** Computer repair generalists typically use off-the-shelf commercial software that is pre-programmed and able to recover what it is designed to find, such as simple deletes or master file or allocation table corruption. If attempts at recovery are limited to this method with no specific knowledge of what is being sought, suspect data may never be detected.

**B. Evidentiary** Simple and advanced recoveries performed without appropriate procedures may corrupt rules of evidence and render what eventually is recovered as inadmissible.

**Protection and preservation of original data** Computer evidence can be one of the most fragile of legal evidence. In an attempt to recovery data for any application, an incorrect method used to investigate the evidence may in some cases destroy the very information sought. In the case of forensics evidence, even if the data is successfully recovered, inappropriate manipulation, storage and transfer of digital evidence may result in an evidentiary challenge to its authenticity.

**Proper transfer, storage and chain of custody** The generally accepted practice of computer imaging, a non-invasive process to copy an entire media source is a very important step to ensure proper recovery and transfer of evidence. An image file requires very specialized software tools and programming skills to also ensure all information is captured.

**C. Data recovery** and **forensics services** can be classified into three categories of:

- basic recovery
- forensic investigative services
- advanced recovery and litigation support

**1. Basic recovery and forensic services** appear to be a growing industry among providers of general IT services. There are a variety of software packages that are effective in recovering data when a drive partition table, boot record, master file table, FAT or root directory is lost or corrupt. These generally occur when a virus has hit, files are deleted or a drive is formatted or "fdisk'ed" or struck by a power failure. Basic computer foren-

[2] Media device OEMs claim, electronic saves are virtually permanent because the platters and oxides that hold the data are typically warranted for 56 years. The mechanical systems and controllers that 'drive' the storage systems are typically warranted for only 2-3 years. Smart users may know how to induce failure while many others may think they know how but really do not. When building a case an investigator needs to know the difference in the case he or she is pursuing

[3] Think of what would happen if you took a deck of cards and threw them FACE DOWN on the floor. Finding specific cards on the floor without an index is similar to what occurs if computer system tries to find a data file when its filing system is damaged, improperly formatted or erased.

sics services provide more sophisticated software repair and often combine these basic data repairs with proper investigative and evidentiary procedures.

**2. Advanced recovery** services are an investigator's best hope to ensure that every possible measure is taken to retrieve data and protect its integrity in a legal case. There are many SW technicians that know how to affect basic data recovery such as simple deletes, but few experienced, qualified technicians that can provide advanced recovery services.

| Basic Recovery | Forensic Services | Advanced Recovery |
|---|---|---|
| Commercial disk repair software packages | Commercial disk repair and advanced forensic SW | Commercial disk repair, advanced forensic SW and advanced programmer and HW diagnostics services |
| Re-image HDD (*sometimes*) | Re-image HDD | Re-image HDD |
| FAT, master file, directory repair | FAT, master file, directory repair | FAT, master file, directory repair |
| Simple Un-Deletes | Simple Un-Deletes | Simple Un-Deletes |
| | Data Capture | Data Capture |
| | Do not corrupt original drive/data | Do not corrupt original drive/data |
| | Proper Evidentiary Trail | Proper Evidentiary Trail |
| | Investigative expertise, i.e. Fraud, accounting, legal | |
| | Expert testimony – technical and specialized investigative | Expert testimony – technical |
| | Password encryption breaking | Password encryption breaking |
| | | Extensive knowledge of what/where to look; what diagnostics to perform |
| | | **Determine IF a failure is HW or SW related** |
| | | Repair/read severely physically damaged hardware |
| | | Read/format obsolete/ outdated media |

**Table 1. Recovery services comparisons**

In the case of more sophisticated data corruption, it is necessary that a data repair technician have the knowledge of not only basic operating systems and widely used application

software, but also understand the structure of these systems and know how to determine a structure of a privately developed SW package.

Most importantly, many data failures exhibit similar symptoms when caused by either a hardware or software problem. It is important that a recovery technician have the right diagnostics tools to determine the true cause of the failure.

**2. Expert testimony of recovery technicians** Discovery and analysis may have to be performed to provide evidence of culpability, such as matching time and date stamps when data is erased or modified.

| Basic Recovery | Forensics | Advanced Recovery |
|---|---|---|
| Generally not available | Tend to be specific SW experts | Expert in all SW packages |
| | Formal and continuing training | Formal and continuing training |
| | | Expert in non-standard software |
| | | Programming AND engineering backgrounds |
| | | Can go to programming source, rather than rely on interfacing |

**Transfer, storage, chain of custody or conversion from outdated storage media** Correctly recognizing the causes, symptoms and effects of data failure that occur in the general sense is an important part of advanced data recovery. General knowledge of common data failures allows an investigator to decide which type of data recovery is needed and what questions to ask a data recovery expert concerning legal forensics.

## IV. Case Studies

Data recovery for litigation or evidentiary support is a procedure to recovery digital evidence caused by an induced failure and/or an attempt to hide or obfuscate evidence. Depending on severity, loss amount, knowledge of last known backup and criticality, recovery may be affected by transfer or acquisition of damaged or hidden files, or may require an advanced data recovery. Consider the following case studies.

**Case 1. Defendant attempts to induce failure to hide evidence** During divorce proceedings, a wife was suspicious that her spouse may be using a computer for illicit, sexually oriented activities. Believing he could permanently delete the computer evidence of his questionable actions, he reformatted the drive and reloaded the operating system. He then confidently turned the computer over to his wife believing he had 'erased' all of his files permanently. He told his attorney there was no evidence to support his wife's claims.

An advanced data recovery service was able to access the media and reconstruct the 'deleted files' where conventional methods failed.

The advanced recovery technicians "found":

1. pornographic web sites,
2. E-Mail messages to girlfriends, and

3. Outlook calendar appointments made with girlfriends.

All of this evidence was assumed to be non-existent by both the husband and the conventional repair technician who first examined the computer. The recovered files were handed over to the client and her legal counsel. The divorce case was settled in her favor without a trial.

Among the lessons learned by attorney, civil wrong doer and conventional PC technician were that a recovery should not be limited to conventional PC repair methods or PC basic recovery, the technology exists to effectively 'undo' deletes and reformats and an evidence 'paper trail' could be determined.

**Case 2. Attempt to use manipulated electronic evidence to defraud.** A user of a service provider's tracking software pressed a $ 15 MM lawsuit against a Fortune 100 company. Citing negligence plaintiff charged:

1. installation of the software in question had permanently damaged/erased his existing files,
2. the data, most of it irreplaceable, not recoverable by any means, and
3. not only could he not access his irreplaceable data, he could not access what files were left in a specific software application critical to running his business.

Concerned the company might in fact be liable, chief counsel with advice from the company's IT director considered settling with the plaintiff and doing a complete review or re-write of the company's software.

Before making a final decision, the company attorney decided to try an advanced data recovery service to determine if his company was liable or if that liability could be mitigated. This "last resort" process had multiple and unexpected positive outcomes for the company.

The first phase of the recovery was able to accurately restore all of the "lost" files and allowed the dismissal of the 2nd charge – the data was unrecoverable.

During a second more advanced phase, programmers were able to restructure and reformat files needed for the claimant's specific software application. The advanced data recovery team was able to reprogram this data when the simple data recovery was not successful, dismissing liability for the 3rd charge – the data once repaired could not be used in a specific software package for the plaintiff to use to run his business.

The third phase of advanced forensic analysis, using electronic data discovery, forensic and analysis applications revealed that the SW installation had nothing to do with the lost data (further rejecting the 1st charge), and determined the plaintiff had manually erased the alleged lost data.

The plaintiff dropped his case and the defendant could have pursued criminal charges against their accuser but settled for an out-of-court settlement to cover legal and data recovery costs.

**Case 3. Attempt to hide the theft of proprietary software.** A programmer and security expert with ten years experience was hired to develop a company's proprietary software. Eventually, the employee decided to leave the company, but first he made copies of all the relevant files for his own use and deleted all the matching corporate data files. The disgruntled employee first made copies to his laptop, then copied those files to an-

other computer and reformatted the hard drives of his work station, the company server and his laptop, and finally he installed a new operating system on the laptop and the work station.

An advanced data recovery team reviewed and copied an exact image of the company drive, un-deleted the critical files from the image and established an exact deletion date and time. (Deletion date and time matched defendant's "log-in" to his PC and the system server and access to physical facility via his door-access code.)

During depositions, the recovery experts were challenged by the defendant's attorney (the defendant claiming himself to be an expert IT witness) that data of this type "was impossible to recover." During the challenge, the recovery experts were able to prove to both the litigants and the judge that not only was it possible they had proof of the recovery and they could trace the data deletions specifically to the defendant.

The defendant accepted a $40 K judgment against him rather than go to trial. Not only was the plaintiff company able to recover its valuable SW, they were able to use the intentional deletions as evidence against the defendant.

## V. Other Considerations

**A. Recovery from catastrophic physical damage** Whether by accident or with intent, there are cases where plane crashes, fire, arson or floods damage systems which seem to make recovery of electronic evidence impossible. It is important to remember that as long as the platters that hold electronically charged oxides on magnetic media, or 'bumps' and 'dye marks' on CDs are not damaged, there is a good chance that all or some of the data can be recovered.

The figure on the right is an illustration of one of five fire-damaged UNIX server drives literally shoveled out of the debris from large auto dealership.

Since the (plastic-material) backup tapes had been co-located with the server drives and were themselves destroyed, all financial data – inventory, accounts payable and receivable, W-2s, customers and loan information – was destroyed.

Nearly 100% of data from these drives were recovered within <u>three</u> days.

**Figure 7. Fire damaged UNIX drive.**

Had the recovery failed, implications from downtime, potential business or insurance fraud could have been astronomical.

**B. Storage, duplication and conversion of media from outdated tape formats** Improvements in PCs, the explosion of the use of MS Windows and the Y2K phenomena have caused many large data users to move from mainframe to PCs and servers very quickly. Today, litigants may need data:

- that has been stored on "old" mainframe backup tape systems,
- was never converted, and
- was either damaged or supported only by obsolete or unavailable operating systems.

In a recent criminal negligence case a data recovery service was able to successfully recover data from just such an old system.

Three years previous, a truck owned by the plaintiff had hit a car and killed three individuals. The plaintiff's trucking firm had been recording raw data on all vehicle travel tracked with GPS but had saved it on an old "main-frame" computer fed by (now outdated) 9-track data tapes. (The mainframe had been upgraded in 1999 since it was not Y2K compliant.)Data recovery experts were able to isolate from the records of approximately 350 trucks over a 10-year period and the driver in question's travel records over a two-year period, and translate the data to a PC readable format.

In the discovery, acquisition and analysis phases the recovery experts were able to validate the data in question under deposition. Evidence was located and read from tapes that were more than 10 years old and were provided to both sides' attorneys. Both plaintiff and defendant were so satisfied with the data that the case was settled out of court.

Chain of custody. Immediate access to the evidence was provided to both sides of the case and was certified for use as evidence if court proceedings were needed. While the data was being recovered, strict control of the tapes and drives was needed.

**Trends** As with many businesses today the trend in developing storage is to do more with less. The computer, recent great strides in personal and enterprise software and the incredible capability and autonomy that all professions have experienced with new technologies have been a leading factor driving new storage trends.

Growth in the complexity and miniaturization of storage devices will be a large part of this continuing trend. Twenty years ago the amount of data that could be stored on a drive the size of a TV set can now be stored on a small laptop drive. Five years ago, what could be stored on a desktop drive is about one-third of what can be stored on today's laptop drive. In less than five years, most desktop drives will be as small as today's laptop drives and possibly hold two to three times as much data, and what today's small laptop drives hold will fit on a device the size of a key ring.

Another trend is growth in medium and large sized HDD systems. International Data Corporation (IDS) forecast the market growth from 1999 to 2005 would see a doubling of enterprise and medium-size computer system HDD growth – from approximately $3.5 – $4 B in 1999 to $7 B in EACH class, much of this growth from devices smaller than today's 3.5" drives.

The recent growth in smaller and more capable devices is accompanied by a rapid growth in problems related to improper storage, failed (or a lack of proper) backups and fraudulently damaged or obfuscated files.

**C. Implications for legal and business** So far we have discussed recovery and its direct implications for the legal community vis-à-vis litigation and support. It would be helpful to consider that in one area – civil or criminal litigation in business cases – the cost of damaged or lost data can be severe.

When involved in cases involving criminal or civil negligence, it is important to have an understanding of the scope of losses that can be directly attributable to the data loss itself. There are over 20 business categories that have been identified as subject to <u>severe</u> business losses when data that drives their mission critical processes has been lost.

The following table lists the PER HOUR cost of downtime by industry.

| Industry Type | Revenue/ Hr ($000s) | Revenue/ Employee |
|---|---|---|
| Energy | 2,817 | 569 |
| Telecommunications | 2,066 | 187 |
| Manufacturing | 1,610 | 134 |
| Financial Institutions | 1,495 | 1,080 |
| Information Technology | 1,344 | 184 |
| Insurance | 1,202 | 371 |
| Retail | 1,107 | 244 |
| Pharmaceuticals | 1,082 | 168 |
| Banking | 997 | 131 |
| Food/beverage processing | 804 | 153 |
| Consumer products | 785 | 128 |
| Chemicals | 704 | 195 |
| Transportation | 669 | 108 |
| Utilities | 643 | 381 |
| Health Care | 636 | 143 |
| Metals/natural resources | 581 | 153 |
| Professional Services | 533 | 100 |
| Electronics | 477 | 75 |
| Construction and engineering | 341 | 216 |
| Media | 331 | 120 |
| Hospitality & Travel | 330 | 330 |
| Average | 979 | 246 |
| Median | 785 | 168 |

**Table 1. The cost of downtime by industry**

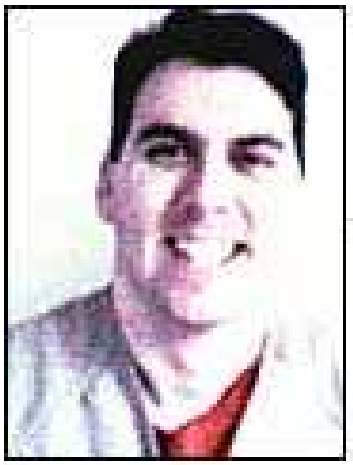
*Source: IT Performance Engineering & Measurement Strategies Oct 2000*

The most important aspect of this section is to realize that data failure occurs often, most times without warning and often times the cost of recovery is more economical than continued downtime.

The recent sentencing of David Smith, author of the 'Melissa' virus, to 20 months has brought this issue to light.

It is estimated that Melissa cost business more than $80 MM in downtime. If one accepts the estimates of researchers that more than half of potential recoveries are not performed, it could be argued that in this case, business losses of $40 MM might have been mitigated if advanced recovery technology were better known.

Many experts claim this is only the beginning of this type of "white collar" sabotage." *(AP, 2002)*



**Convicted: David Smith**

**D. Advanced Data Recovery.** Whether by accident or intent, damage to physical systems can occur that would make investigation of electronic data evidence appear impossible.

It is important to remember that if the platters that hold electronically charged oxides on magnetic disks or tapes, or the CDs that hold "bumps" and "dye marks" are not too damaged, there is a good chance that all or much of the data, hitherto thought to be lost, can be recovered.

There are really only a few highly trained specialists able to perform data recovery and forensics with any level of confidence. And while basic recovery can simple deleted or "lost" files, advanced recovery and proper evidentiary procedures are often needed to advance a case.

Advanced data recovery utilizes the ability to recover data with knowledge of how chain of custody and data contamination procedures effect digital evidence preparation. Computer forensics experts look at *available* digital files with an accountant's, environmentalist's or architect's trained eye, and see information that is incorrect, where mistakes have been made and where information has purposely been falsified.

Consider Al Capone's tax evasion trial – forensic experts looked at his books (both sets of them) to find a money trail to determine that Capone really made more than the $2000 a year he claimed. An advanced data forensic recovery expert, would be able to find the books at the bottom of a river and make them legible, and would be able to show where Capone's accountant erased and replaced certain figures in the ledgers.

Most firms recognized as computer or digital forensic professionals perform simple data retrievals, un-deletes, directory repairs and re-imaging of electronic media. The advanced recovery process goes beyond that to find data likely to be missed using simple recovery and forensics methods.

***Checklist.*** The following is a checklist an investigator might want to consider when developing a case with digital evidence:

Are the services being used to gather electronic evidence exploit:

- a capability to rebuild a damaged media device, such as in a "clean room," and
- large storage capacity for duplication, imaging and conversion of media from outdated to newer or advanced formats?

Can the forensic and programming procedures being used withstand chain of custody or evidential integrity challenges posed in court? Do the experts being used have experience with many types of operations, hardware and file systems and media storage devices:

- Tapes – cassettes, drives -- HDDs, diskettes, CDs and other emerging optical systems
- PCs laptops, servers
- MS/DOS, Macintosh, UNIX, Linux

Because permanent loss of data could occur and have severe consequences a good data recovery specialist should provide timely response with the proper solution. A full service data recovery and forensics services firm knows how to:

- Image the electronic media
- Repair the electronic allocation (FAT) file or tape catalogue
- Discern specifics of a FAT or catalogue damage
- Identify if a file or a FAT has been fragmented
- Physically rebuild a hard drive to get it to spin and access data.

## VI. Summary

Many, who deliberately tamper with data or, try to make it appear that the data has been inadvertently damaged or lost, are relying on the theory that either computer data is permanently "lost" or the false perception that if recovered, data cannot be traceable back to them or their nefarious activities

At the heart of computer forensics recovery are the correct techniques used to retrieve information from electronic systems that:

- can stand the test of evidence,
- may appear to an investigator to be permanently lost or damaged, but is actually still on the media device, and
- may be permanently lost if attempted with the wrong techniques.

A litigant having the basic knowledge of data recovery and forensics, and having an advanced data recovery provider can mean the difference between winning and losing. It may also mean failing to prosecute or defend to the limits of today's technology capability.

Despite the fact that disaster data recovery appears to be of growing concern, there are still only about five companies nationwide that have the experience, the personnel and the capital equipment to do a credible job.

The oldest and the largest advanced data recovery firms are listed below:

| **The oldest** | **The largest** |
|---|---|
| **Data Recovery Services, Inc** | **OnTrack** |
| 2636 Walnut Hill Ln Suite 230 | 9023 Columbine Rd |
| Dallas, TX 75229 | Eden Prairie, MN 55347 |
| 214 350-8202 | 952 937-5161 |
| 877 304 7189 (toll free) | 952 937-5750 |
| www.datarecovery.net | www.ontrack.com |

**About the presenter/author.**

Thomas J Kapurch is a former Intelligence Officer, US Navy and Defense Intelligence Agency, with more than 15 years experience in information systems, intelligence collections, analysis, technical information systems, geo-political intelligence and military investigations.

His industry experience includes over ten years in business and information systems management for GTE, Nextel, NEC America, TXU, Informatica Software Company with 11 years experience developing business and operations plans, as internal and external information systems consultant to telecommunications, utilities and financial companies.

Mr. Kapurch worked as an engineer with Texas Instruments on computer based aerospace products with OEMs and major subcontractors Bell Textron, McDonnell Douglas, Boeing and Lockheed. While at TI, Kapurch also managed all phases of electronics systems and components manufacturing and enterprise wide information systems for manufacturing and shipping.

He is currently Vice-President of Data Recovery Services Inc. in Dallas, Texas, responsible for designing and presenting technology seminars for litigation support and government services.

**Education**

| | |
|---|---|
| BS, Engineering, US Naval Academy, Annapolis, MD | 1975 |
| MBA, University of Dallas, Irving, TX | 1988 |
| MA, Strategic Studies, US Naval War College | 1991 |
| MA, International Relations and Politics | 1991 |

# Section 3b

# Advanced Data Recovery with Forensic Applications

Tom Kapurch
Data Recovery Services, Inc
Dallas, Texas

# Data Recovery

***"Since '92 … computer crime cases sent to federal prosecutors (have) tripled, while the number … actually prosecuted has remained the same.***

***Of … 419 cases referred to prosecutors, only 83 were prosecuted.***

***<u>The rest were dismissed due to lack of evidence</u>."***

***Electronic Privacy Information Center (EPIC)***

***29 January 2001***

# Storage Devices

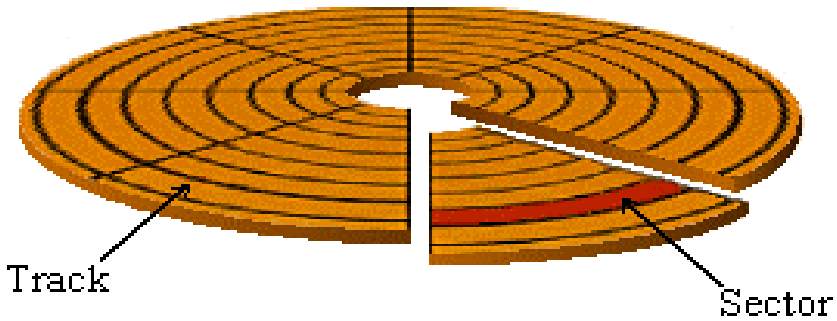
**Stored on 2 general media types**

- **Magnetic**
  - **Tapes, diskettes, hard disk drives (HDDs)**
    - **Rearranged oxides on coated plastic film**
- **Lasers disks**
  - **CDs – CD-Rs and CD-RWs**
    - **Microscopic bumps or burned spots**

# How Data Is Stored

## Magnetic platters resemble vinyl records

- Spin, access w/ device that DOES NOT touch
- Tracks and sectors serve as filing system

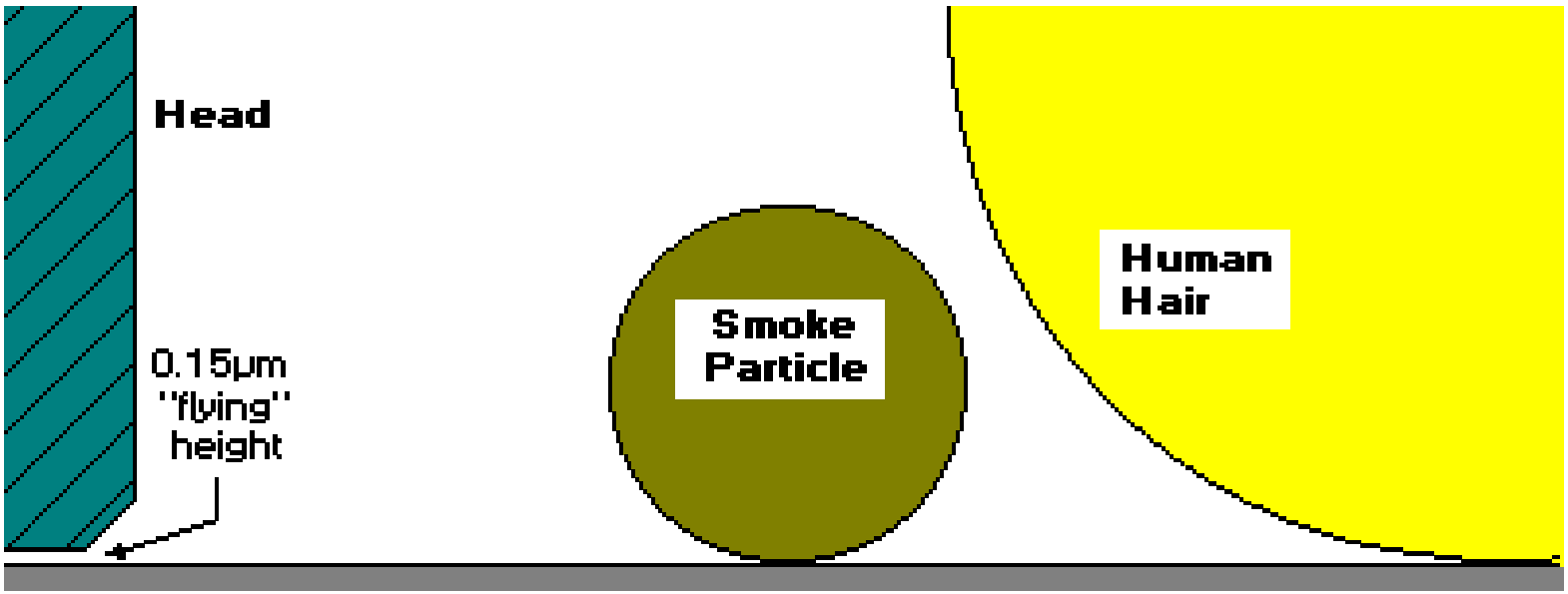



- If data appears lost it <u>may be</u> the system simply can't find the proper track or sector
- Storage media are typically warranted for 60 years!
- The electronics can and often fail within 2-3

# How Data Is Stored

## Media storage sensitivity to damage

## How critical is critical?



# Symptoms and Causes

0100101100101001011101
0010110010100101110111
0100101* 0010100101110
0110110010100101110101
0110010100101110100101
0010100101110101011001
0110010100101110101011
0010100101110101011001
0010010111010101101001
0111010101100110110101
0101001011101010111011
0110010100101110101011

**A Lost Bite = A Lost File**

**Lost File(s) = Lost Evidence**

- **Mechanical failure**
- **Earthquake, flood, fire, electrical**
- **Normal or abnormal wear**
- **Drive fails to spin or makes a clicking sound**
- **Caused by spin motor, surface damage, contamination, scratches**

# Implications

**‘Smart’ users know how to induce failure**

- **Mechanical or SW failure can appear similar, oftentimes misdiagnosed**
- **In building a case an investigator may not realize the evidence still exists**

**<u>Wrong-doers bank on this likelihood</u>**

# Basic / Forensics / Advanced Recovery

- Basic recovery techniques recover for which standard SW is designed to look
- Forensic experts look at data that's *available*
  - With an accountant's, environmental expert's or architect's trained eye
- Advanced recovery determines cause of failure
  - HW or SW – repair severely physically damaged HW
  - Determine what/how data was changed/ deleted/damaged

# Civil Litigation

**Citing negligence, user claims:**

- SW installation permanently erased files
- Irreplaceable data not recoverable
- Files critical to specific applications unusable

**Data recovered**

- Dismiss 2nd claim – data was unrecoverable

**Reprogrammed so applications worked**

- Dismiss 3rd claim – repaired "unusable" data

**Discovery and analysis**

- Dismiss 1st claim – SW installation had not affected data
- Determined the user *purposefully* erased data

$15 MM suit dropped, *could* have pursued criminal

# Criminal Litigation

**Paid to develop SW, programmer departs**

- Copies, deletes matching corporate files
- Reformats drives
- Installs new OS

**Un-delete critical, partially written over files**

- Establish exact deletion time and date

- Deposed, defendant challenges: “impossible to recover”
- Recovery expert counters
  - Convinces litigants, judge deletions traced to defendant
  - Existence of recovered SW used against defendant
  - Plaintiff company recovers proprietary SW
  - Plaintiff accepts $40K judgment

# Implications for Legal and Business

- **$MMs in lost opportunity or business costs yearly**

  **PER HOUR cost of downtime by industry (Top 5)**

  - **Energy $2,800**
  - **Telecommunications 2,100**
  - **Manufacturing 1,600**
  - **Financial 1,500**
  - **IT services 1,300**

- **50% of lost data cases go unresolved, in large part due to fact IT managers and end-users are unaware or untrained in data recovery technology**

***Source: IT Performance Engineering & Measurement Strategies, Meta Group Oct 2000***

# Implications for Security

- Terrorists are at threshold of using Internet
- FBI officials: multiple "cyber casings" of US sites, routed through telecommunications switches in Saudi Arabia, Indonesia and Pakistan
  - "Casing" emergency systems, electrical generation, transmission, water storage and distribution, nuclear power plants and gas facilities
- Commercial digital controls for infrastructure designed with fewer safeguards than on-line pizza purchase sites
- Banking and securities companies slow to see threat and have little to counter cyber disruption

*Wash Post 27 June 02*

# Implications for Security

- Case remains a tough sell.
  - Banks, brokerages, most security-conscious, do not tell when systems are attacked
  - Gov't did not learn details about Nimda worm, caused $530 MM in damage, until stricken companies fired security executives
  - Companies worry about loss of customer confidence, legal liability when they report flaws
  - FBI has little success w/ key initiative to identify most dangerous points of vulnerability in 5,700 companies deemed essential to national security

*Wash Post 27 June 02*