Data Management and Security:

The Solution to eDiscovery and Compliance

By Robert F. Copple, J.D., Ph.D.

Data Management and Security

! Evolution to Electronic Data Storage

- Pre Internet and Electronic Storage
  - Paper Document Storage
    - Difficult, Expense, Haphazard
- Tended to Limit
  - Storage
  - Access
  - Compilation & Analysis

Data Management and Security

!Electronic Data Storage Changed Approach to Document Storage

- The IT Professional's Dream
  - Cheap and Easy
  - No Reason to Cull Files
  - Save Everything
  - Crunch, Compile and Analyze Everything

- The Result
  - Greatly Increased Volume of Data Saved By Businesses

Data Management and Security

!Sensitive Data Is Replicated and Spread Across The System

- More Potential Sources for Documents
  - Central Servers
  - Specific Network Servers
  - Backup Tapes and Systems
  - Local Hard Drives
  - PST Drives
  - Email Accounts
  - Thumbdrives, Portable Drives, Cell Phones . . . .

Data Management and Security

! Potential Business Nightmare

- **IT Costs**
  - Increased Storage Capacity
  - Additional Drain on IT Resources
  - Enhanced Security Requirements

- **Legal and Compliance Costs**
  - Liability and Penalties
  - Remedial Measures
  - Customer Trust and Loyalty

Data Management and Security

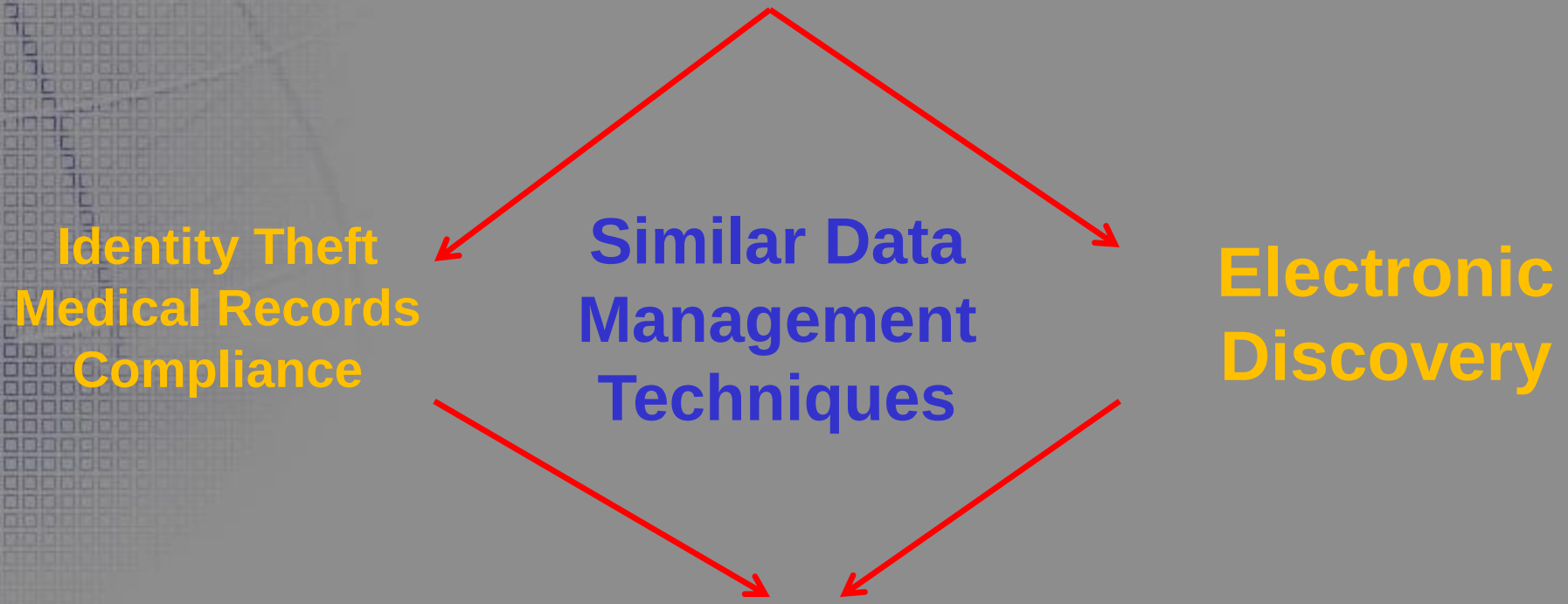
eDiscovery -- A Litigation Management Nightmare

- Discovery Costs
  - Greatly Increased
  - Discovery as Litigation Leverage

- Shift in Strategy and Litigation Gamesmanship
  - Spoliation and Sanctions
    - More Documents + More Sources = Greater Probability
    - Intentional Setup

Data Management and Security

Electronic Data Management



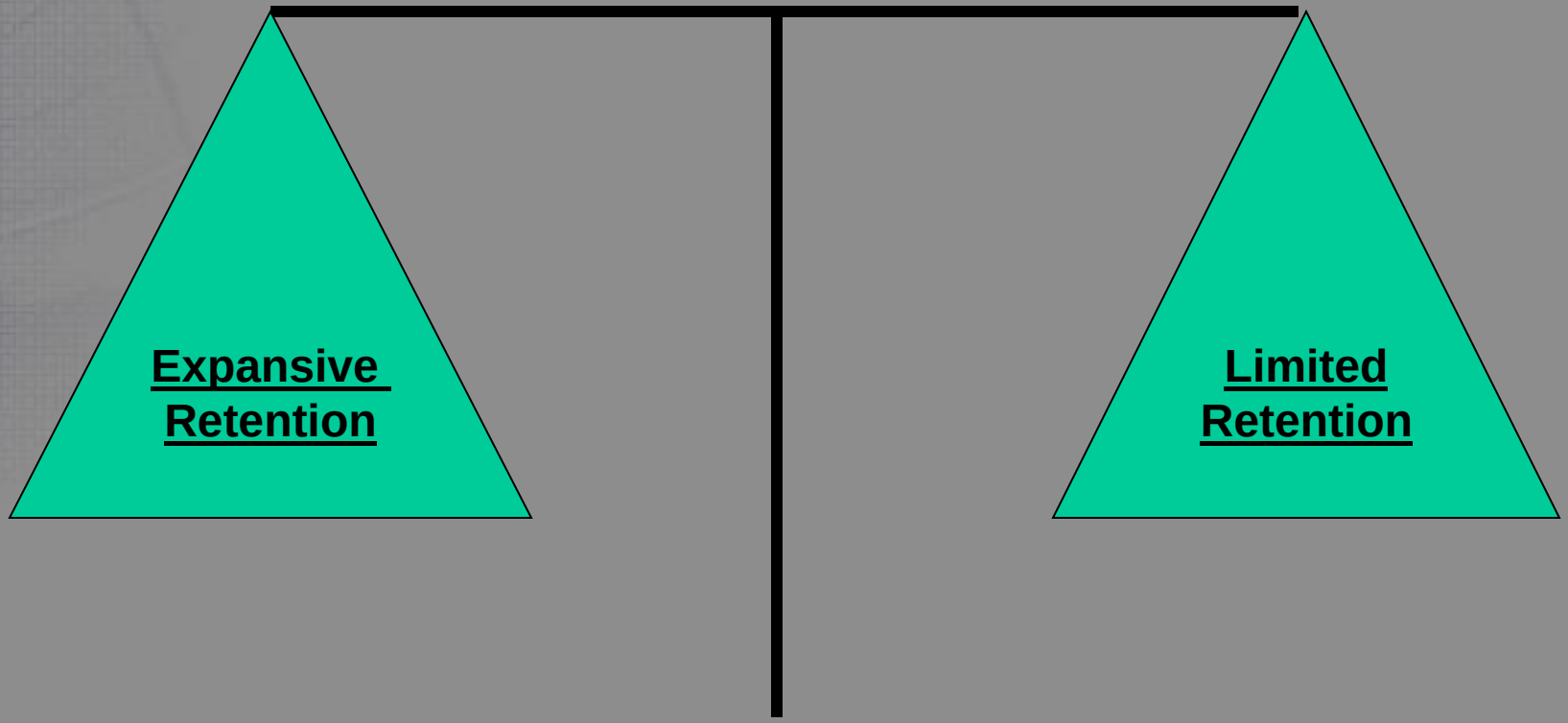
Effective Business Solutions

Data Management and Security

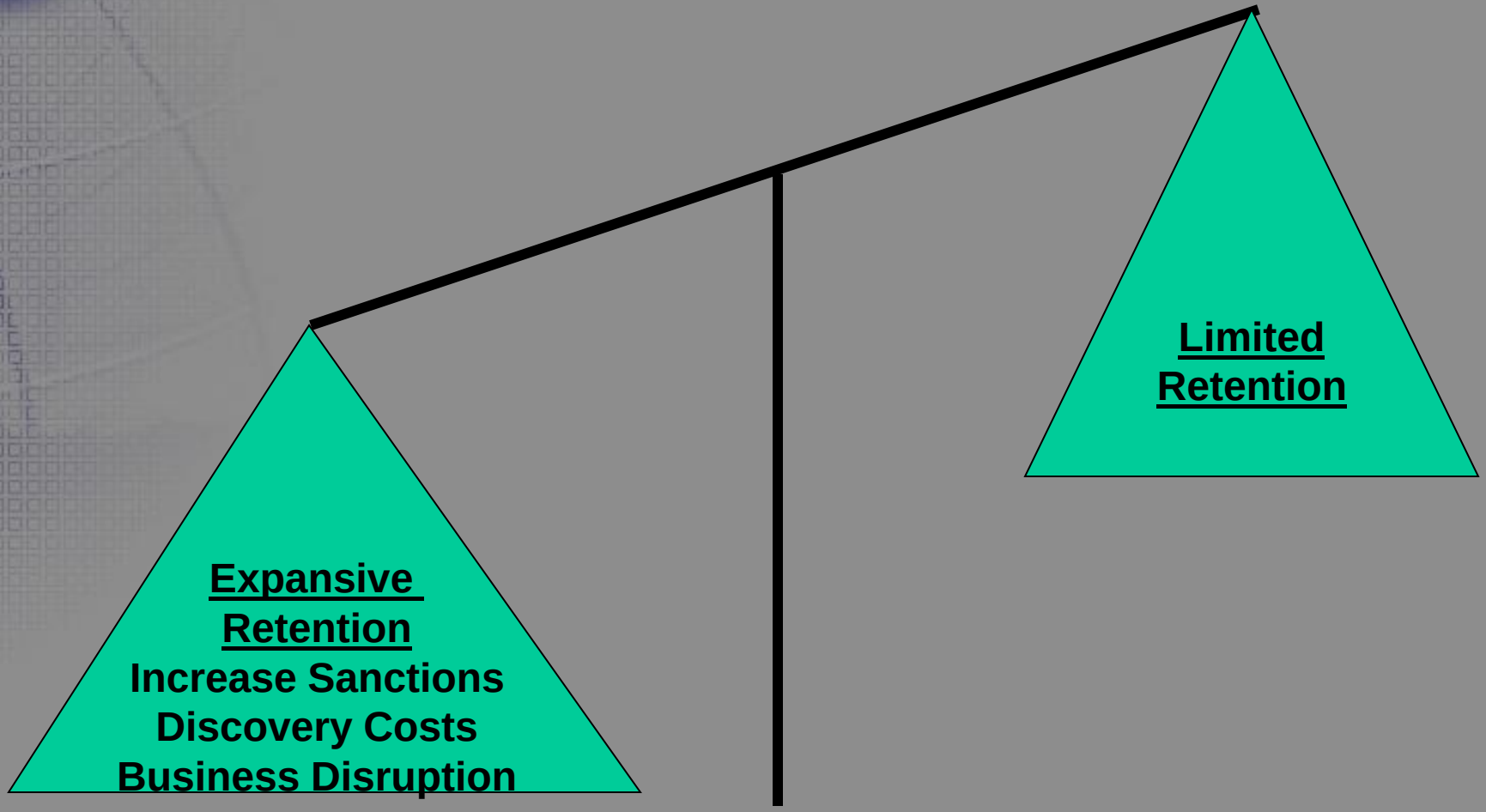
Data Management Policy -- Three Goals

- Retain records necessary to business operations.
- Promote the efficient use of information technology ("IT") resources.
- Retain those records required to satisfy legal obligations

Data Management and Security



Data Management and Security



Data Management and Security

Data Management Policy: Guideline #1: Know What Data You Collect And Why

- **The Data Inventory – Know:**
  - **What Data You Collect**
  - **Why You Collect it**
  - **Where you store it**
  - **Who Has Access**

- **Types of Collected Data:**
  - **General – Credit Card & Social Security Numbers**
  - **Specific – HIPAA, SEC Reporting, Financial, Litigation**

Data Management and Security

Data Management Policy: Guideline #2: Documents Should Be Discarded Unless There is a Good Business or Legal Reason to Retain

- Limit
  - What You Keep
  - How Long You Keep It
- Avoid The Tendency To Keep Everything
- Make Informed Choices About What To Keep
  - Data Important To Business Operations
  - Data Related To Compliance and/or Litigation

Data Management and Security

Data Management Policy: Guideline # 3: Dispose Of Data No Longer Needed

- Systematic Deletion Process
- Pursuant To Data Management Policy
- Use Automated IT Tools When Possible
  - Methods And Examples

- Exceptions:
  - Financial Documents
  - Insurance Policies – Liability / Occurrence
  - Regulatory Documents – Corporate, Tax, Environmental
  - Employment – Statute of Limitations
  - Personally Identifiable Information

Data Management and Security

Data Management Policy: Guideline # 4:

Policy Must Be Simple and Easy To Implement

- Limit Number of Subject Matter Categories
- Limit Number of Time Period Categories

- **Policy Must Be Tailored to Business Needs and IT Capabilities**

Data Management and Security

Identity Theft Protection Policy: Guideline #5: Consistently Implement And Enforce Your Policy

- Use Automated Systems and Behavioral Controls
- Establish Expectations
- Motivate Compliance
- Policy As A Condition Of Employment
- Employee Agreement
- Training

- **Inconsistency Will Create a Taint of Intentional Spoliation**
- **Policy Without Proper Implementation Worse Than No Policy At All**

Data Management and Security

Problem Areas: The 80/20 Rule

- Email
- Texting and Instant Messaging
- Local Hard Drives
- PST Drives
- Home Computers
- Cell Phones / Blackberries
- Mothballed Servers – Lingering Files
- Backup Tapes
- Paper Documents / Off Site Storage

Data Management and Security

Identity Theft and Personally Identifiable Information

- FTC Rule
- Additional Security and Access Requirements

Data Management and Security

RFCopple Articles And Presentations On Data Security And eDiscovery

Electronic Discovery in Arbitration, Alternative Dispute Resolution Section, Arizona State Bar Association, February 5, 2008.

Management of Electronic Data Under the European Union Directives and the Federal Trade Commission Rules, Phoenix, Arizona, November 17, 2004. Live Webcast Sponsored by the State Bar of Arizona.

Defensive Data Management: The Best Way To Protect Your Electronic Information, Phoenix, Arizona, November 10, 2004. Live Webcast Sponsored by the State Bar of Arizona.

An Effective Document Retention Policy: Your Best Defense to Electronic Discovery, Lewis and Roca, Business Litigation Seminar Series, March 17, 2004.

Data Management and Security

RFCopple Articles And Presentations On Data Security And eDiscovery continued

Discover New E-worlds, Legal Times, (April 21, 2008).

eDiscovery: It's All About the Information, Arizona ADR Forum, (Fall 2007).

Dealing With Data: No, You Can't Call Them Documents Anymore, Business Law Today (March-April 2005).

Firms Must Pick Which Data To Save, Arizona Republic (September12, 2004).

Data Life Cycle Management, ACCA Docket (September 2004).