

Records and Information Management and Retention

June 28, 2011

Greater Washington Society of CPAs
Not-for-Profit Organizations Committee
Washington, DC

W. Warren Hamel

Venable LLP

750 E. Pratt St.

Baltimore, MD 21201

410-244-7563

Melissa Gomez

Venable LLP

575 7th Street, N.W.

Washington, D.C. 20004

202-344-4381



“Why Should I care about Records and Information Management?”

Records and Information Management is a tool to manage the **costs** of storage of records and maintenance of electronic information, and the **risks** associated with either (a) not having records that are legally required to be retained, or (b) maintaining records that could have been destroyed or deleted pursuant to a Records and Information Management policy.



Forbes' "Wall Street Fine Tracker"
(http://www.forbes.com/2002/10/24/cx_aw_1024fine.html)

Goldman Sachs, Morgan Stanley, Citigroup, Deutsche Bank, U.S. Bancorp Fined \$8.25 million

- **"Dec. 3, 2002 | Goldman Sachs, Morgan Stanley, the Salomon Smith Barney unit of Citigroup, the Deutsche Bank Securities unit of Deutsche Bank and the U.S. Bancorp Piper Jaffray unit of U.S. Bancorp each agreed to pay \$1.65 million in fines for allegedly violating e-mail record-keeping requirements. The fines were assessed to each company by the SEC, the New York Stock Exchange and the NASD. In accepting the penalties, the broker-dealers neither admit nor deny the allegations."**



“Morgan Stanley offers \$15M fine for e-mail violations: Firm was under SEC investigation for failing to save e-mails”

- **February 14, 2006** ([Reuters](#)) -- NEW YORK -- U.S. investment bank Morgan Stanley has offered to pay \$15 million to resolve an investigation by U.S. regulators into its failure to retain e-mail messages, according to a regulatory filing. The Wall Street firm said it had reached "an agreement in principle" with the U.S. Securities and Exchange Commission's Division of Enforcement to resolve an investigation into its preservation of e-mails. The fine would be one of the largest penalties ever imposed on a Wall Street firm for failing to preserve records.
U.S. market regulators had threatened to fine Morgan Stanley for failing to keep e-mails in several recent cases brought against the brokerage.



“NASD Fines Four Fidelity-Affiliated Broker-Dealers \$3.75 Million for Registration, Supervision and Email Retention Violations”

Feb. 5, 2007 NASD press release

- NASD announced on February 5, 2007 that it had fined four Boston-based Fidelity broker-dealers a total of **\$3.75 million** for improperly maintaining NASD registrations for 1,100 individuals, failing to assign registered supervisors to 1,000 individuals, **failing to retain the email of 1,900 registered individuals**, and **other electronic recordkeeping failures**. NASD also ordered the four broker-dealers to conduct comprehensive audits of the firms' systems, policies and procedures relating to registration and electronic recordkeeping.



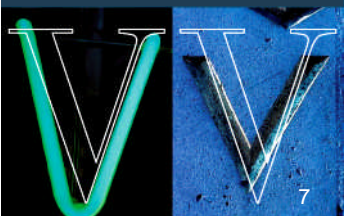
Qualcomm v. Broadcom, 2008 U.S. Dist. LEXIS 911 (Jan. 7, 2008)

- Qualcomm ordered to pay Broadcom's attorneys' fees and litigation costs -- **\$8.6 million**
- Six outside lawyers for Qualcomm referred to California Bar Association
- Outside lawyers plus Qualcomm and 5 in-house attorneys ordered to take part in Case Review and Enforcement of Discovery Obligations ("CREDO") program



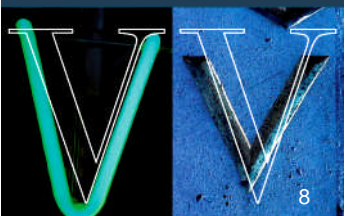
Benefits of a Comprehensive RIM Policy:

1. A robust RIM Policy and Procedure ensures that records that are needed for business purposes are organized and retained;
2. How much is your organization spending on storage of hard copy records? What is the cost of maintaining servers or back-up tapes for electronic information that you no longer need? A RIM Policy permits a company to discard unnecessary records and reduce storage costs;



Benefits of a Comprehensive RIM Policy:

3. Ensures that treatment and retention of records and electronic information are consistent throughout the company;
4. Shields the company against claims of spoliation, bad faith or obstruction of justice when records are demanded in litigation or in a government investigation;



Benefits of a Comprehensive RIM Policy:

5. Lowers production costs when records have to be produced;
6. Can have a positive return on investment by streamlining and rationalizing work flow.



Risks of Operating without a Record Retention Policy



Risks include:

- Retaining documents unnecessarily
- Heightened liability in civil litigation
- Diminished credibility in government investigations
- Fines and Sanctions for Failure to Retain Documents when Necessary



Slide 10

A3

ADDED THIS SLIDE TO DRIVE HOME THE BOTTOM LINE POINT EARLY ON: your org NEEDS a RIM policy - everyday you operate w/out one you are losing \$ not to mention all the financial risks you are placing the org in - we will expand further throughout the presentation

What do u think?

Administrator, 6/26/2011

The Records and Information Managemetn Policy: Shield or Sword?

U.S. v. Arthur Andersen

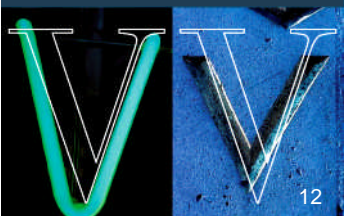
- Arthur Andersen accounting firm convicted in connection with collapse of Enron and firm's shredding of documents prior to receiving an SEC subpoena
- Although case was overturned on appeal by the U.S. Supreme Court, Arthur Andersen was destroyed by prosecution



***Arthur Andersen v. United States*, 125 S. Ct. 2129, 2135 (2005)**

United State Supreme Court recognized the prevalence of document management policies and the legitimacy, under normal circumstances, of using them to ensure the destruction of certain information.

A RIM Policy must be comprehensive, neutral and tied to legitimate business requirements and legal principles.



What is a Document Management Policy?

Records and Electronic Information Management (RIM) Policy

- A document management policy consists of a management program that:
 - Defines company records;
 - Provides how long specific types of records should be maintained;
 - Gives instructions for disposing of certain records; and
 - Establishes procedures for ensuring compliance with the policy.



Situations Requiring the Production of Records:

Before things “go wrong”—

DUE DILIGENCE

**Don’t wait for the lawsuit,
subpoena or investigation**



Government Requests Requiring the Production of Records:

- Government investigations
 - EEOC requests;
 - Taxing authority requests; and
 - Regulatory agency investigations
- Government requests can take the form of administrative subpoenas and grand jury subpoenas.



Civil Litigation Requires the Production of Records:

- Civil lawsuits
 - Product liability cases;
 - Commercial disputes;
 - Discrimination claims;
 - Securities litigation

- Requests in Litigation can take the form of Requests for Production of Documents and Interrogatories.



Categories of Records

- Courts generally expect companies to keep records certain categories of records, such as:
 - Products made;
 - Services provided;
 - Employees;
 - Financial affairs;
 - Corporate operations; and
 - Previous claims and lawsuits.



Example: Employee Records

- Sources of federal law related to employee records:
 - Fair Labor Standards Act of 1938 (FLSA)
 - Equal Pay Act
 - Employee Retirement Income Security Act of 1974 (ERISA)
 - Summary plans, reports on benefit plans
 - Title VII of the Civil Rights Act of 1964
 - Americans With Disabilities Act (ADA)
 - Age Discrimination in Employment Act of 1967 (ADEA)
 - Occupational Safety and Health Act of 1970 (OSHA)
 - Log and summary of occupational injuries and illnesses
 - Family and Medical Leave Act of 1993 (FMLA)



When Document Management Policies Go Wrong

The Consequences of Destroying Too Much or Too Little

Administrative Sanctions

Civil Sanctions

Criminal Sanctions



Consequences in Civil Cases

Courts May Sanction a Party with One or More of Several Punitive Measures:

- “Spoliation Inference”
 - Fines
- Bar a Party from Making an Argument or Introducing Evidence
- Default Judgement or Dismissal of Case



Other Consequences in Civil Cases

Court may chastise counsel or impose sanctions on counsel. Or ... **punish the corporation in lieu of disciplining the attorney.**



Metropolitan Opera Ass'n, Inc. v. Local 100,
2004 WL 1943099 (S.D.N.Y Aug. 27, 2004)

- ◆ Decision to impose sanctions was not based upon whether the documents were relevant, but, instead based upon the "vexatious manner" in which the defendants failed to comply with discovery. The court stated that the "defendants and their counsel may not engage in parallel, know-nothing, do-nothing, head-in-the sand behavior in an effort to consciously avoid knowledge of or responsibility for their discovery obligations and to obstruct plaintiff's wholly appropriate efforts to prepare its case."



Pension Comm. of Univ. of Montreal Pension Plan v. Bank of Am. Secs., LLC, 2010 WL 184312 (S.D.N.Y. Jan. 15, 2010)

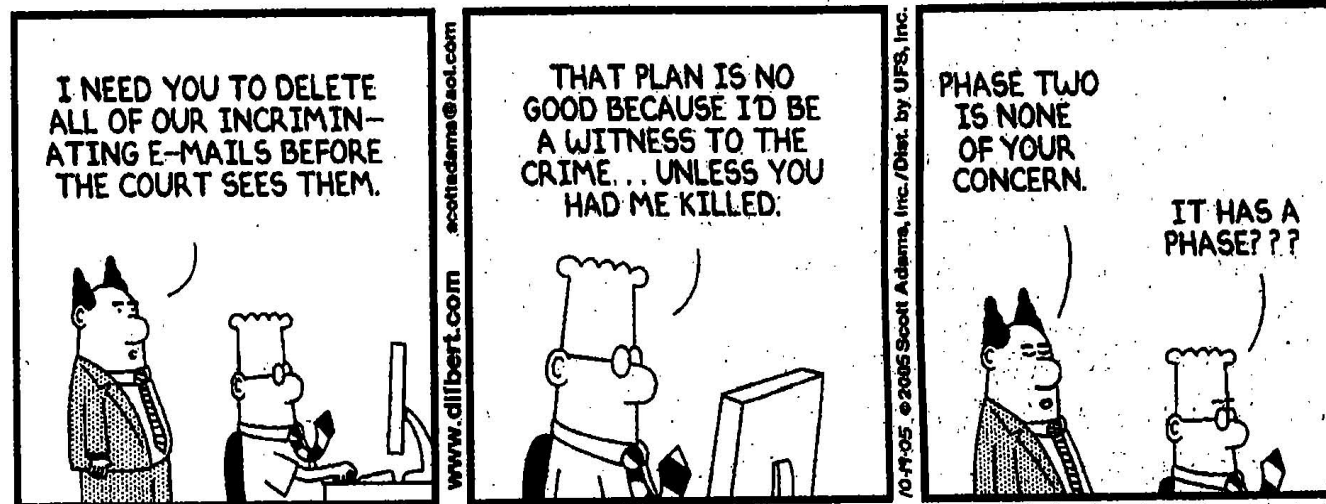
- Judge Schiendlin's latest opinion serves to remind us that e-discovery sanctions remain a serious threat. Judge Schiendlin stated: "By now, it should be abundantly clear that the duty to preserve means what it says and that a failure to preserve records-paper or electronic-and to search in the right places for those records, will inevitably result in the spoliation of evidence."

The court specifically identified several actions (or failures to act) which would result in a finding of gross negligence in upholding discovery obligations:

- Thus, after the final relevant *Zubulake* opinion in July, 2004, the following failures support a finding of gross negligence, when the duty to preserve has attached: to issue a written litigation hold; to identify all of the key players and to ensure that their electronic and paper records are preserved; to cease the deletion of email or to preserve the records of former employees that are in a party's possession, custody, or control; and to preserve backup tapes when they are the sole source of relevant information or when they relate to key players, if the relevant information maintained by those players is not obtainable from readily accessible sources.



■ DILBERT[®] by Scott Adams



*When Document Destruction Goes
Criminal:
United States v. Arthur Andersen*

**Arthur Andersen charged under 18 United States
Code Sec. 1512(b)(2)(B) “Corrupt Persuader”
theory in a federal criminal case.**

**Core allegation was the destruction of documents
sought by SEC and DOJ.**



Alteration or Destruction of Records 18 U.S.C. Sec.1519

Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct or influence the investigation or proper administration of **any matter within the jurisdiction of any department or agency of the United States . . . or in relation to or contemplation of any such matter or case . . .** [shall be guilty of a crime].



Consequences of *Not* Destroying Documents Pursuant to Policy

Document Retention Policies are *risk management tools*. Once a policy is in place, a firm should make every effort to comply with the policy.

In some instances, litigants have increased liability by failure to destroy documents as called for by the Records Management Policy.



RECORD-KEEPING DURING LITIGATION:

Duty to Preserve

*Discovery under the Amended Federal Rules of Civil
Procedure*



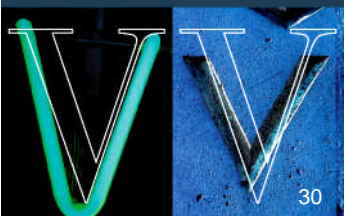
Duty to Preserve

- A legal obligation to preserve evidence occurs upon notice that litigation might occur. *Renda Marine v. United States*, 58 Fed. Cl. 57 (Fed. Cl. 2003).
- Duty to preserve arises **at the latest with service of the complaint**, and counsel has a duty to advise client of pending litigation and the need to preserve potentially relevant documents.
- Most companies are aware of the potential for litigation before it starts, e.g., demand letter, preservation letter, threat to sue.



Texas v. City of Frisco, 2008 WL 828055 (E.D. Tex. Mar. 27, 2008)

- State of Texas sought a declaratory judgment relieving them from a general preservation request from the City of Frisco.
- Preservation request asked the Texas DOT to preserve all electronic data associated with a specific toll project that might become the subject of environmental litigation
- The State asked the Court to determine whether the pre-suit request violated Rules 26(f) and 34
- Court declined to make such a determination or to issue an advisory opinion as to what would constitute good faith by either side in handling their Rule 37 good faith preservation obligations



Suspending the Destruction Schedule

- Suspend your document destruction schedule for all relevant documents as soon as you anticipate:
 - Civil litigation
 - A criminal or regulatory investigation
- Notify individual employees of litigation that relates to them, and instruct them to preserve whatever information they have that relates to the case.



Remember to Include Electronic Records in Your Legal Hold

- Remember to suspend the destruction of electronic records, especially records generated or maintained by witnesses and custodians.
- Remember automatic purge programs that destroy e-documents.



Initiate...

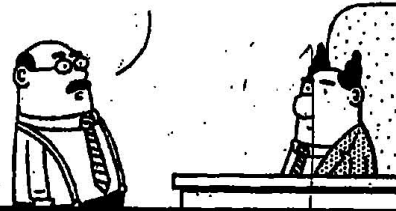
- Archiving of electronic documents once litigation begins.
- Contact with outside technological and legal consultants who are experienced in electronic discovery.



DILBERT BY SCOTT ADAMS

COMPANY LAWYER

THE COURT ORDERED
US TO TURN OVER ALL
OF OUR E-MAIL
RECORDS.



www.dilbert.com scottadams@aol.com

GOSH. I SURE HOPE
THEY DON'T GET
DELETED DURING
REGULARLY SCHEDULED
SYSTEM MAINTENANCE.



10-18-05 ©2005 Scott Adams, Inc./Dist. by UPS, Inc.

OH NO.
THAT
WOULD
BE BAD!
WINK!
WINK!



GOOD GRIEF,
MAN! HOW
CAN YOU BE
FLIRTING AT
A TIME LIKE
THIS?



***DISCOVERY UNDER THE CURRENT
FEDERAL RULES OF CIVIL
PROCEDURE***

- E-discovery changes took effect on December 1, 2006
- Changes cover 5 main areas



- Early meet and confer (Rules 16 and 26)
- Claw back for inadvertent production (Rule 26(b)(5)(B) and 26(f))
- Searching ESI to answer interrogatories (Rule 33(d))
- Production of ESI (Rule 34)
 - ESI that is not reasonably accessible need not be produced absent good cause showing by requestor
 - Very recent cases and legislative proposals (California, Canada) focusing less on accessibility and more on “good cause” and “marginal utility” as the standard
- Safe harbor for routine destruction of ESI (Rule 37)



Williams v. Sprint/United Mgmt Co. (D. Kan. Sept.29, 2005)

- ◆ Production of electronic data must include metadata unless party objects or seeks protective order; sanctions possible for failure to produce.



Identifying ESI for possible review and production

- Is information stored on firm devices that might need to be produced?
- Divide the question into two categories:
 - Potential records created by humans
 - Potential records created by the device



Human-generated Records

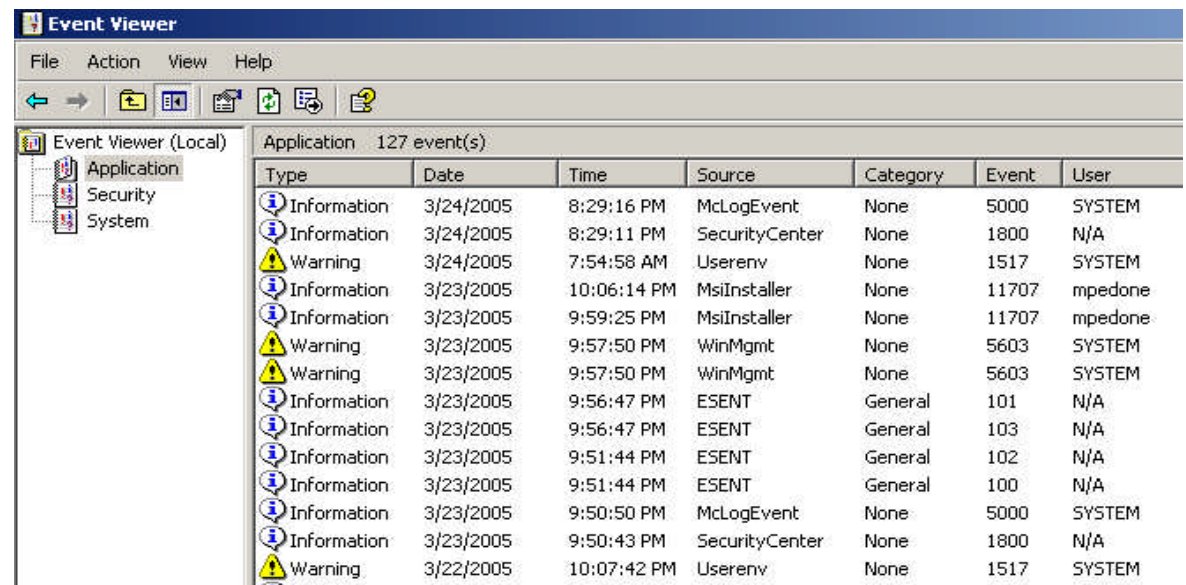
- Word processing documents, spreadsheets
- Database files
- Electronic mail messages
- Organizer items (calendar entries, etc.)
- Text messages
- Metadata
- Application-specific data, e.g.:
 - Accounting journal entries
 - Shipping records, etc.

...these are just examples



Device-generated records

- Less obvious to the non-techie
- Most common form is a log
 - Activity
 - Error



The screenshot shows the Windows Event Viewer window. The left pane displays the 'Event Viewer (Local)' tree with 'Application', 'Security', and 'System' logs. The right pane shows a list of 127 events. The table below represents the data visible in the right pane.

Type	Date	Time	Source	Category	Event	User
Information	3/24/2005	8:29:16 PM	McLogEvent	None	5000	SYSTEM
Information	3/24/2005	8:29:11 PM	SecurityCenter	None	1800	N/A
Warning	3/24/2005	7:54:58 AM	Userenv	None	1517	SYSTEM
Information	3/23/2005	10:06:14 PM	MsiInstaller	None	11707	mpedone
Information	3/23/2005	9:59:25 PM	MsiInstaller	None	11707	mpedone
Warning	3/23/2005	9:57:50 PM	WinMgmt	None	5603	SYSTEM
Warning	3/23/2005	9:57:50 PM	WinMgmt	None	5603	SYSTEM
Information	3/23/2005	9:56:47 PM	ESENT	General	101	N/A
Information	3/23/2005	9:56:47 PM	ESENT	General	103	N/A
Information	3/23/2005	9:51:44 PM	ESENT	General	102	N/A
Information	3/23/2005	9:51:44 PM	ESENT	General	100	N/A
Information	3/23/2005	9:50:50 PM	McLogEvent	None	5000	SYSTEM
Information	3/23/2005	9:50:43 PM	SecurityCenter	None	1800	N/A
Warning	3/22/2005	10:07:42 PM	Userenv	None	1517	SYSTEM



Columbia Pictures Indus. v. Bunnell, et al. (C.D. Cal., May 29, 2007)

- Defendants ordered to begin capturing and preserving Internet Protocol ("IP") addresses processed by their computer servers that were temporarily stored in random access memory ("RAM")
- Court rejected argument that this sort of data was ephemeral and thus incapable of being preserved



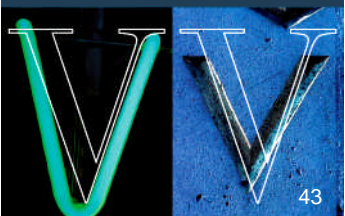
New Types of Electronic Records

- Are new technologies creating new “records”?
- Yes – consider:
 - Instant messaging
 - Cell phone text / image messages
 - Blogs
 - Wikis
 - Corporate virtual worlds (e.g., on SL)
- What’s next???



Retention of Electronic Records

- Adopt RIM Policy that addresses Electronically Stored Information (ESI)
- ESI is no different than hard copy records, except in terms of format and how it is stored
- Promote centralized data management
- Establish sensible backup procedures (i.e., system disaster recovery back-up tapes are NOT an appropriate means for record retention)



Me? I thought YOU had the tapes...

“Just after lunch on May 2, [Time Warner] employees received an e-mail from the company’s chief security officer explaining that the company had **lost backup tapes** bearing names and Social Security numbers of about 600,000 current and past employees, as well as some of their beneficiaries.”

“Time Warner Loses Employees’ Data”
Fortune – May 2, 2005

Note: In fairness to Time Warner, it appears the tapes were lost by an outside vendor who was supposed to store them.



*Safeguarding Individuals and
Your Company From Liability
and Criminal Charges By
Adopting a Robust Corporate
and Electronic Information
Management Policy*



Steps for Implementing a Document Management Program

- (1) Create a document management committee made up of senior management and attorneys or with attorney counsel.
- (2) Inventory the types of company records by department. May wish to use a Record Inventory questionnaire, or in some cases, work with an outside consultant.



Steps for Implementing a Document Management Program

- (3) Develop an inventory form addressing:
- Title/description/category of record;
 - Content;
 - Employees responsible for maintaining the record;
 - Location;
 - Recommended retention period;
 - Purpose of retention; and
 - Whether the record is an original or a copy.



Steps for Implementing a Document Management Program

- (4) Collaborate with an attorney with experience in records management policies and procedures to draft a Records and Information Management Policy for committee review and approval.
- (5) Have senior management review and approve the Policy.



Steps for Implementing a Document Management Program

- (6) Formally adopt the Policy: Does this need a Board resolution, or can it be adopted by management as part of internal controls?.
- (7) Distribute the Policy to managers throughout the company.



Steps for Implementing a Document Management Program

- (8) Train employees and managers to implement the Policy.
- (9) Make “process changes” (storage, offsite storage, IT procedures, draft and approve document management documents) to implement the Policy.
- (10) Consider whether records management software that works concurrently with the organization’s retention policy is appropriate for your organization.



Training

Emphasize the Cost Savings

Emphasize the Management of Risk

Emphasize Cleaning the Work Space

“Make it Fun”



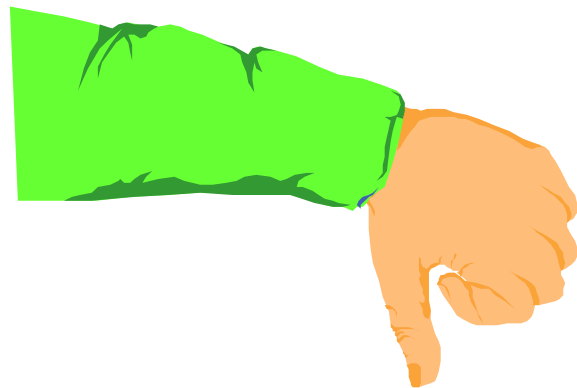
BLONDIE YOUNG & LEBRUN

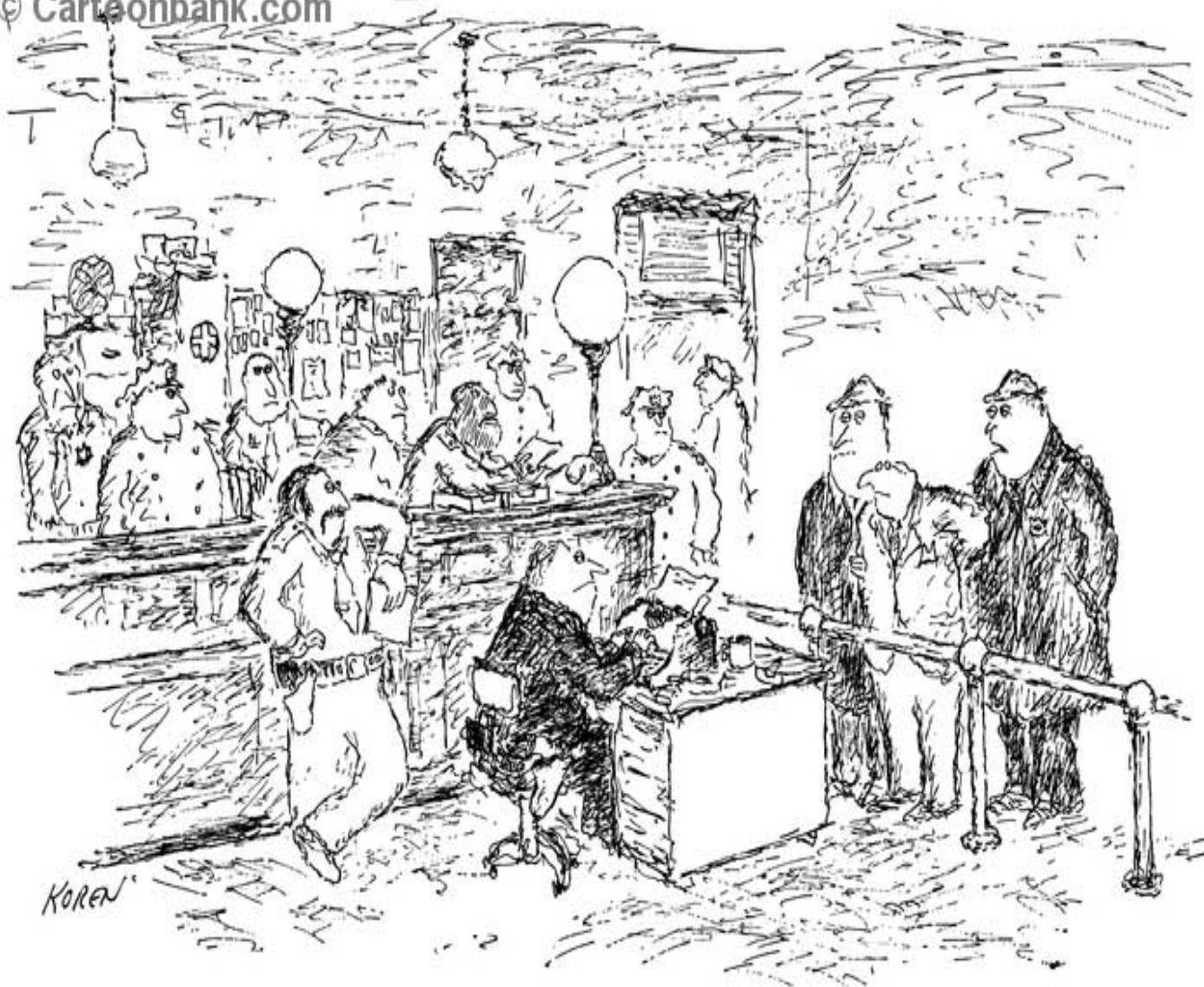


Training

If all else fails ...

**Threaten them with Disciplinary Action
for Non-Compliance.**





"He's charged with expressing contempt for data-processing."

“Information governance” now a
key component in corporate
compliance and ethics
programs



**For Example:
Federal Sentencing Guidelines Amendments
*Organization's Compliance & Ethics (C&E)
Program***

Maintaining an “effective compliance and ethics program” requires Organization to:

- Exercise ***due diligence*** to ***prevent and detect*** criminal conduct; and
- Otherwise promote an ***organizational culture*** that encourages ethical conduct and a commitment to compliance with the law. Sec. 8B2.1(a)



Records and Information Management and Retention

June 28, 2011

W. Warren Hamel

Venable LLP

750 E. Pratt St.

Baltimore, MD 21201

410-244-7563

Melissa Gomez

Venable LLP

575 7th Street, N.W.

Washington, D.C. 20004

202-344-4381

