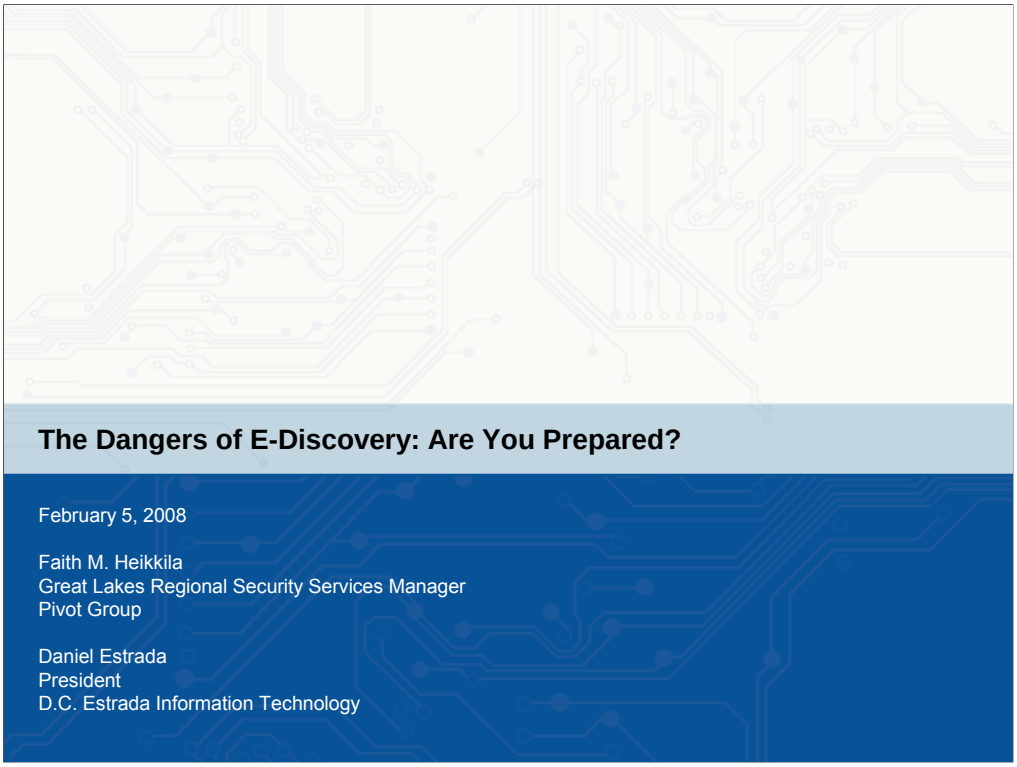


Faith M. Heikkila

Previously worked as a complex litigation paralegal and IT Project Manager for 18 years:

- Varnum, Riddering, Schmidt & Howlett
- Miller, Canfield, Paddock & Stone

I am not a lawyer and I do not even play one on TV.

This presentation is:

- merely my opinion
- does not constitute legal advice

Please contact your attorney for legal advice relevant to your e-discovery needs.

Faith's research interests include secure remote access to organization databases, information security policies/procedures, and privacy issues. Heikkila is a member of the ACM, the Association of Information Technology Professionals (AITP), the Computer Security Institute (CSI), the IEEE, InfraGard, the Information Systems Security Association (ISSA), and ConnecTech Greater Kalamazoo (formerly known as Great Lakes Interactive Marketing Association-Southwest).

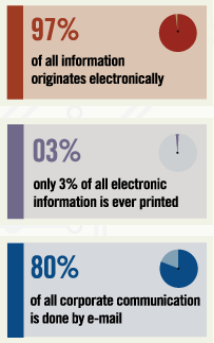
Faith is currently a PhD candidate in information systems, specializing in information assurance, at Nova Southeastern University. Contact her at fheikkila@pivotgroup.net.

Why Do E-Discovery?

Discovery with a Twist: ESI (2005)
- 97% of information originates electronically
- 3% is ever printed
- 80% of corporate communication: e-mail

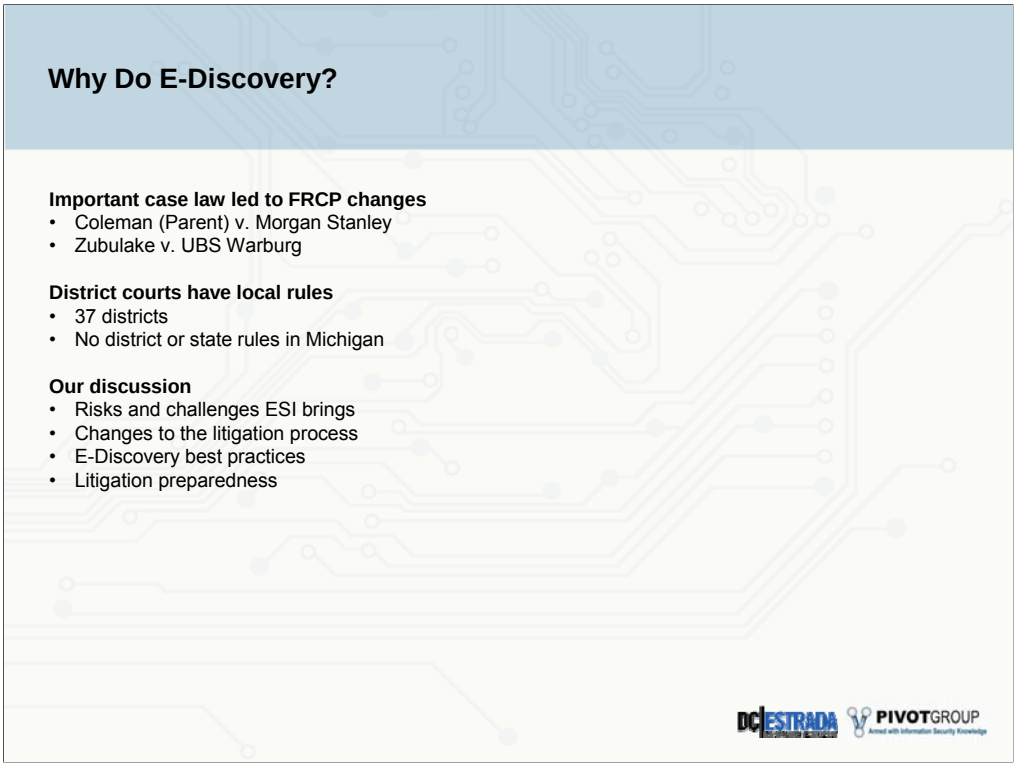
- Paper is not enough
- Validated by case law, rule changes

Companies Unprepared (June 2007)
- 69% not ready to respond to litigation
- 51% not yet identified anyone in IT to testify
- 9% legal has provided clear guidance
- 6% confident in immediately handling e-discovery requests



Sources: Radicati Group, Contoural/Osterman Research Survey

Notes:© Faith M. Heikkila, Pivot Group



The case of ***Coleman v. Morgan Stanley*** (2005 WL 679071), however, caught the attention of law firms. In this case, the jury awarded in excess of $1 billion to the plaintiff based on the mishandling of backup tapes by Morgan Stanley and their counsel. The court held that Morgan Stanley had been stonewalling and attempting to hide their e-mail, thereby violating numerous discovery orders (March 1, 2005 Order).

In the court's order, Morgan Stanley's attorneys were blamed for not having adequate knowledge about the ESI of their client. Thus, the new e-discovery rules provide motivation for communicating with clients' IT personnel at the early stages of the case to discuss data (evidence) preservation, the types of ESI under the client's control, whether the data is accessible and inaccessible, and the costs associated with producing inaccessible ESI.

The new rules stem from recent opinions, starting with the Laura Zubulake's gender discrimination and retaliation case (***Zubulake v. UBS Warburg, LLC***) against her former bank employer. In one of five decisions, the court shifted the cost of discovery to Zubulake for retrieval of the data from backup tapes (*ZUBULAKE I*).

However, when the judge later opined that the bank had failed to preserve electronic evidence and instructed the jury to assume the lost e-mail messages would be unfavorable to the bank, the cost for this production was charged back to the bank (*ZUBULAKE V*). In April 2005, the jury found for Zubulake, and she was awarded $29.3 million in damages primarily because the bank had failed to adequately preserve evidence.

Notes:© Faith M. Heikkila, Pivot Group

How ESI Changes Litigation :

Discovery process has changed significantly
- New discovery requirements
  - *New questions for client / organization (see E-Discovery Guide)*
  - *Adequate follow-ups are critical*

How costs are handled
- Typically: each side pays for its costs
- Cost shifting is possible
- "Undue burden or cost" standard

Traditional paper production
- Manual review
- Bates stamping
- Redaction

- Scanning with OCR/OWR is an option

Electronic production
- Native or non-native (PDF/TIFF) formats
- Search capabilities
- Electronic numbering and redaction

DC ESTRADA PIVOTGROUP

There must be convincing evidence that the production of these types of ESI would be overly burdensome.

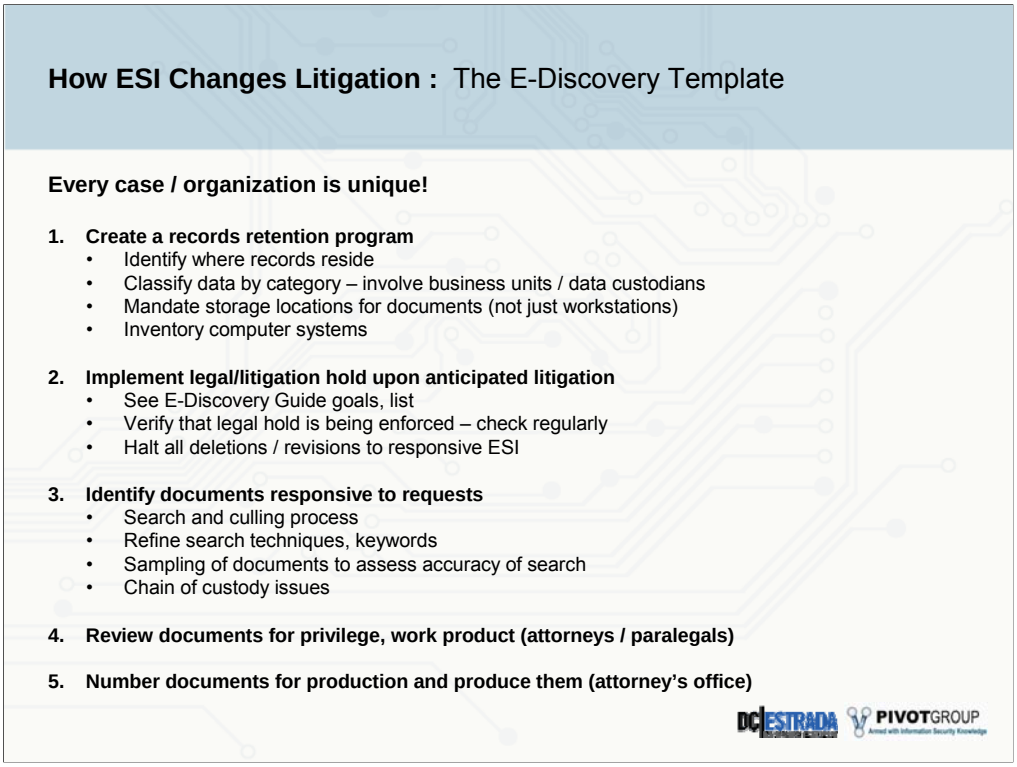
If the magnitude of procedures needed to extract the ESI is not compelling, the federal judge may order the information be produced with the burden of the cost to be absorbed by the producing party.

The paper review took months to review millions of documents. Faith worked on a complex litigation cases that had 15 million and 21 million documents exchanged during the discovery phase of the lawsuits. The 15 million document case was during the paper production and there were 3 shifts of 100 people inputting data into a database and bates stamping (placing a unique number on each document in order to identify it and produce it as an exhibit in court) each document. Redaction included blacking out content that was attorney-client privileged or protected by the work product doctrine.

Optical Character Recognition (OCR) and Optical Word Recognition (OWR) were two of the techniques used to scan documents into databases in the earlier years of document productions. The issue was that OCR recognized about 86% of the characters meaning that 14 out of every 100 letters were not recognizable. This lead to a lot of clean up in trying to make actual words out of those letters that were not recognized.

Electronically produced documents are much easier to handle, although there are a lot more of them making ESI more voluminous productions. The ability to search information in native format has become necessary, especially if the information does not make sense without the metadata (i.e., Excel spreadsheet formulas).

Notes:© Faith M. Heikkila, Pivot Group

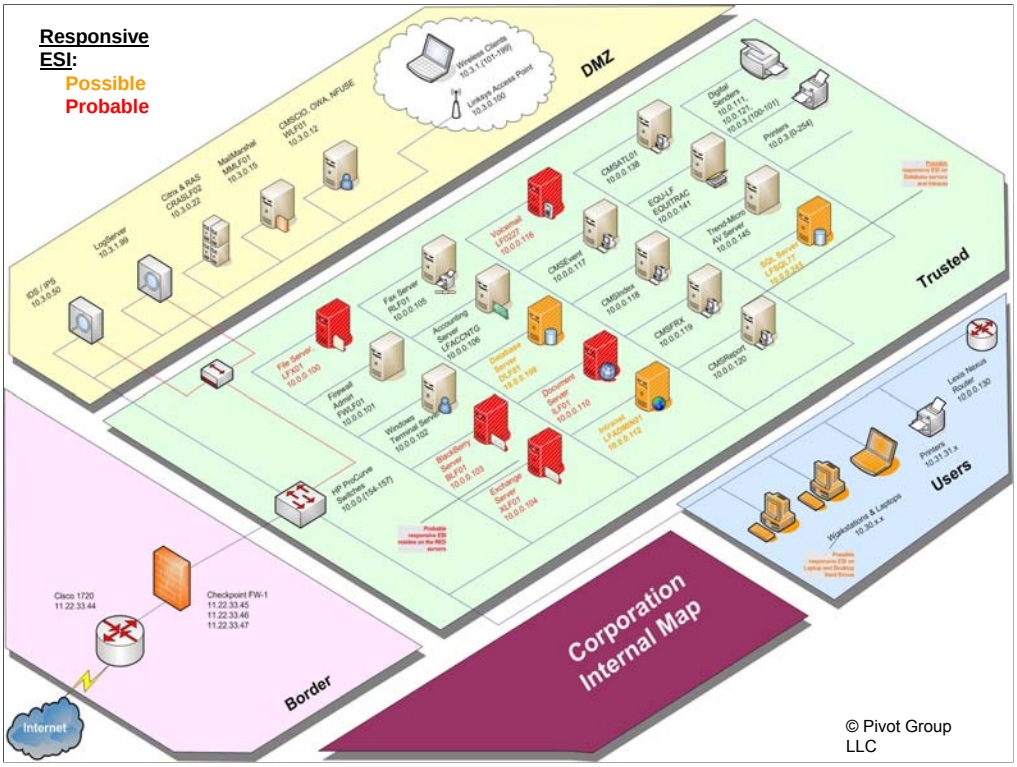


According to O'Neill, Behre, & Nergaard (2007), the development of a litigation response protocol should include:

1. **A template should include definitions of all documents and data to be preserved!**
2. **The procedure for retaining such documents and data**
3. **The method of distribution to and acknowledgement of receipt by employees – frequency of re-distribution of the litigation hold instruction.**
4. **Required distribution list for all litigation hold instructions – IT and HR with a protocol for identifying other appropriate data custodians.**
5. **Plan for identifying relevant sources of ESI and halting the regular retention schedule for this information.**

O'Neill, M. E., Behre, K. D., & Nergaard, A. W. (2007, February). New e-discovery rules: How companies should prepare. *Intellectual Property & Technology Law Journal, 19*(2), 13-16.

Notes:© Faith M. Heikkila, Pivot Group



During the e-discovery phase called the meet and confer, attorneys need to know the location(s) of their clients' responsive ESI and what the economic impact of paying for the production of inaccessible documents will be for their client.

Visio Network Diagram: "A picture paints a thousand words." Become familiar with a program that will produce a network diagram showing where the data resides. This document will be extremely beneficial as an exhibit to the meet and confer report filed for the scheduling conference.

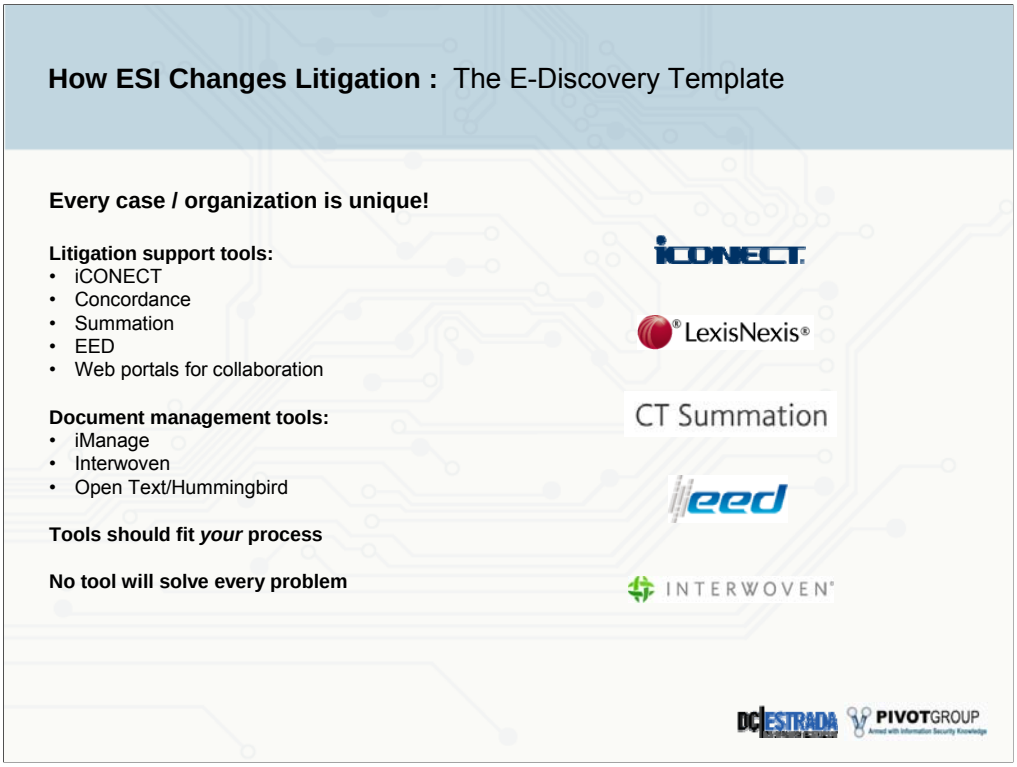
Perform a network assessment to produce a network architecture diagram illustrating where data resides.

The court is forcing a proactive review of the production of ESI by determining upfront whether the case merits the expense of retrieving inaccessible ESI. One way to clearly identify where possible and/or probable ESI resides is to use a network map. In a corporation with enterprise servers, ESI can be on a number of different servers such as:

1. files servers
2. Blackberry servers
3. exchange servers
4. document servers
5. voicemail servers
6. database servers
7. SQL servers,
8. or any number of other servers.

Also, ESI can be stored on workstation hard drives, laptops, or removable media devices.

Notes:© Faith M. Heikkila, Pivot Group



Notes:© Faith M. Heikkila, Pivot Group

How ESI Changes the Role of IT :

Preservation and retention efforts are different
- "Reasonably foreseeable litigation" standard
- Coleman case example

Increasing storage requirements
- More data must be preserved
- Storage is relatively inexpensive, but implementation is not
- IT budgets are tight
- Archival may make sense

- When choosing storage solution:
  1. Cost / benefit of in-house v. off-site
  2. Investigate security, security history
  3. Assess cost and ease of accessing data

Don't forget opportunity cost: staff, delays in litigation

Notes:© Faith M. Heikkila, Pivot Group

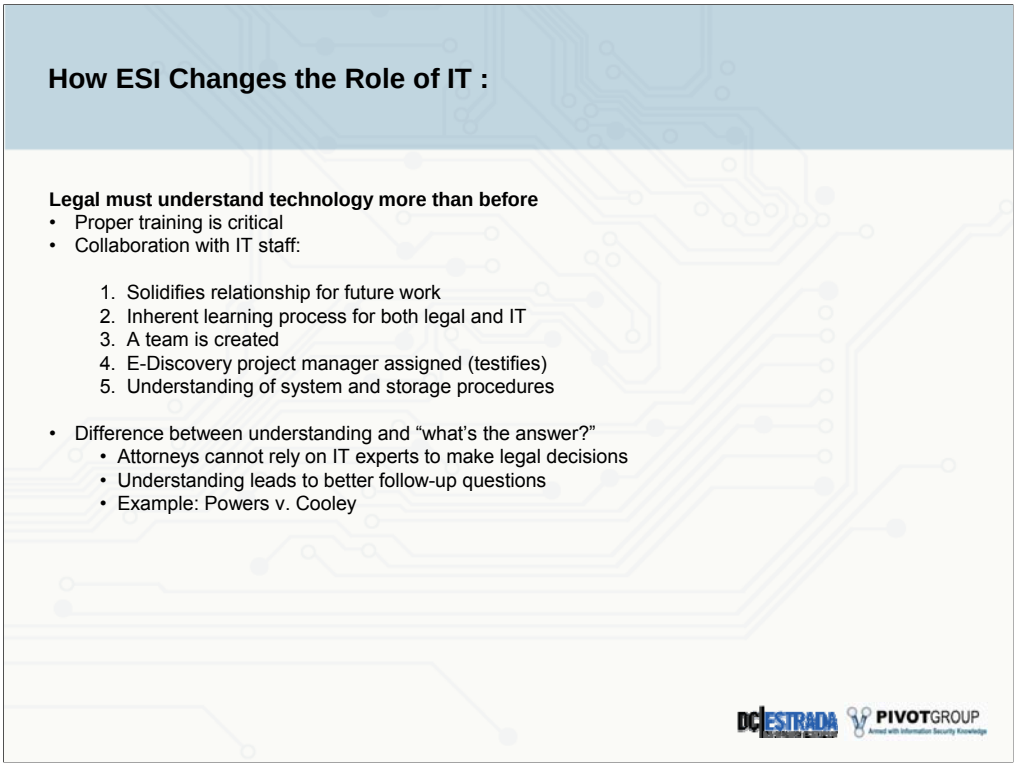
How ESI Changes the Role of IT :

More storage = more to collect and review

- In-house search tools for large organizations
- Easy access to data important for all organizations
  - backup tapes
  - e-mail archives
  - VoIP systems
  - instant messaging

***Many* more devices, formats, access methods:**

Notes:© Faith M. Heikkila, Pivot Group



Local Judge in W.D. of Michigan Decision

Powers v Thomas M. Cooley Law School, **Lexis 67706 (W.D. Mich., Sept. 21, 2006) (Mag. Joseph G. Scoville)**

Denied Motion: Defendant's Help Desk computerized work system could not be imaged or reviewed

Plaintiff was visually impaired and claims her ADA computer malfunctioned during her final examinations.

Defendant upgraded from the "Track It" system to the "HelpStar" system during the discovery time period.

Defendant's IT Dept. produced paper tickets during the overlapping two month period to the satisfaction of the Court.

Plaintiff's counsel failed to request an order compelling the review of Defendant's computers in writing

Notes:© Faith M. Heikkila, Pivot Group

How ESI Changes the Role of IT :

IT people must understand legal requirements, goals

Goals of Legal:	Goals of IT:
Minimizing exposure and risk Reducing cost of litigation Anticipating worst-case scenario Implementing legal holds Producing responsive documents Redacting privileged / work-product	Making IT work Keeping IT running Data classification and organization Enforcing legal holds Proper storage / deletion procedures Planning future IT growth?

When is e-discovery necessary?

- When the parties agree
- When the important stuff is not on paper
- When the court orders it

Notes:© Faith M. Heikkila, Pivot Group

E-Discovery Risks and Dangers :

The "smoking gun"
- Greatest challenge
- Find client's and opposing party's

High cost and burden to the organization
- Time spent on legal holds
- Time spent locating / identifying responsive ESI
- Third-party costs: outside counsel, tools, experts
- Data classification issues

Bad publicity (skeletons released)
- Don't be the next "poster child"

Inability to produce responsive ESI (possible sanctions)
- Legacy systems and backups – not retrievable

Inadvertent waiver of privilege / release of secrets or work product
- Metadata
- Needle in a haystack: high volume of data
- Related challenges: privilege may not exist

  Example: Scott v. Beth Israel Medical Center

DC ESTRADA PIVOTGROUP

See: *Dr. W. Norman Scott v Beth Israel Medical Center Inc., and Continuum Health Partners Inc.,* Supreme Court of the State of New York, County of New York: Commercial Division, Index No. 60273 6/04, October 18, 2007.

Plaintiff sued his employer for breach of contract. Plaintiff used the company e-mail to communicate with his attorney. Since the company had a policy stating that no communications through the company e-mail system were private, Beth Israel was able to obtain copies of his e-mails. Relying on the company's policy, the Court agreed that there was no attorney-client privilege attached since there was no expectation of privacy when using the employers' e-mail system.

Local Judge in W.D. of Michigan Decision

***Thielen v Buongiorno USA, Inc.* Lexis 8998 (W.D. Mich., Feb. 8, 2007) (Mag. Judge Brenneman)**
Ordered Plaintiff's computer be produced for inspection by third party expert without parties or attorneys present.
Imaged the hard drive to see if Plaintiff had opted-in for a subscription to entertainment content.
Allowed Plaintiff's counsel to review expert's findings prior to giving to Defendants
- •with ten (10) days to object or
- •request a Protective Order for any findings

Notes:© Faith M. Heikkila, Pivot Group

Handling E-Discovery Complexity :

Be Realistic – don't take on too much!

Treat e-discovery like complex litigation
- Break into functional parts
- Assign time, attorney, or team to each part
- Rely on the decisions made for each part
- Review the big picture, how everything fits together

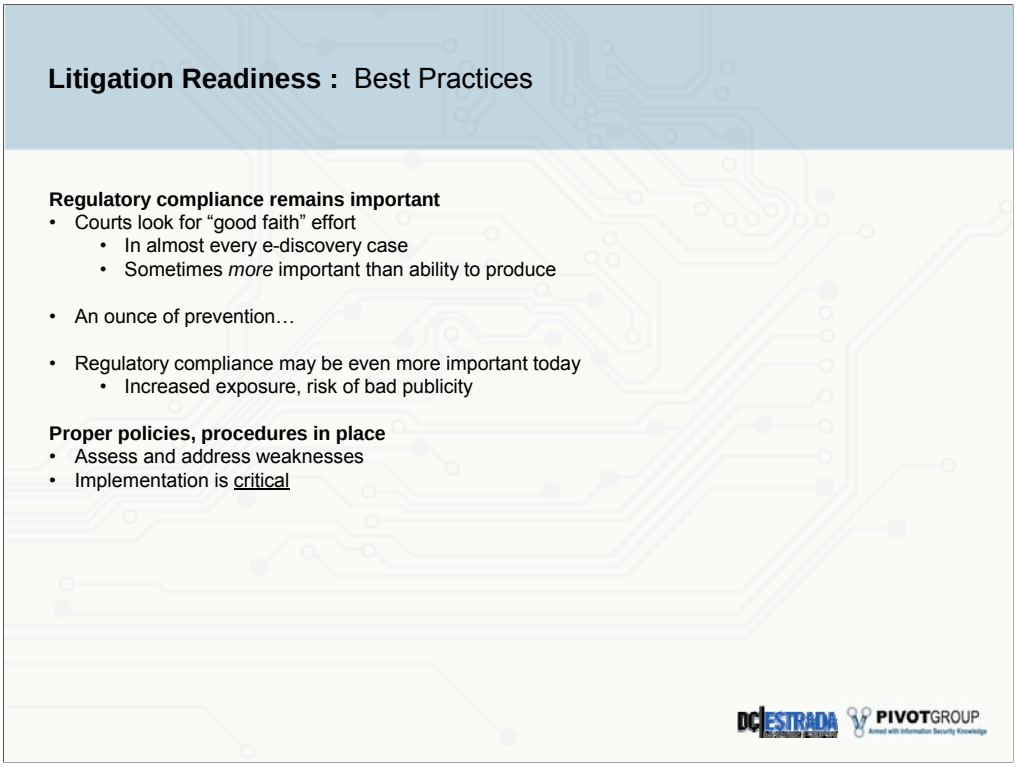
Fear is the greatest adversary
- Technology is not untouchable
- Legal professionals don't have to be IT experts
- Basic understanding goes a long way

  Example: Great American Ins. v. Lowry Development

Legal pros must understand questions
- Courts do not accept IT illiteracy
- Experts do not replace understanding
- Should rely on experts for specific details
- More effective counsel
- Follow-up questions are vital

DC ESTRADA PIVOTGROUP

Notes:© Faith M. Heikkila, Pivot Group



SOX – applies to public companies (not to law firms)

GLBA – applies to financial institutions (not to law firms – lawyers regulated by State Bar Association and ABA). GLB financial institutions have to incorporate disposal policies to abide by mandated safeguards.

HIPAA – Business Associate Agreement --- how long holding onto data and destruction procedures. Privacy of medical information. This information is generally encrypted to protect it. Must protect sensitive data from inadvertent exposure during the case.

Violation of HIPAA is a violation of the ethical obligations of a lawyer.

Fair Credit Reporting Act (FCRA) and **Fair Accurate Credit Transactions Act (FACTA)** – Must take reasonable measures to dispose of sensitive information from credit reports and backgrounds checks.

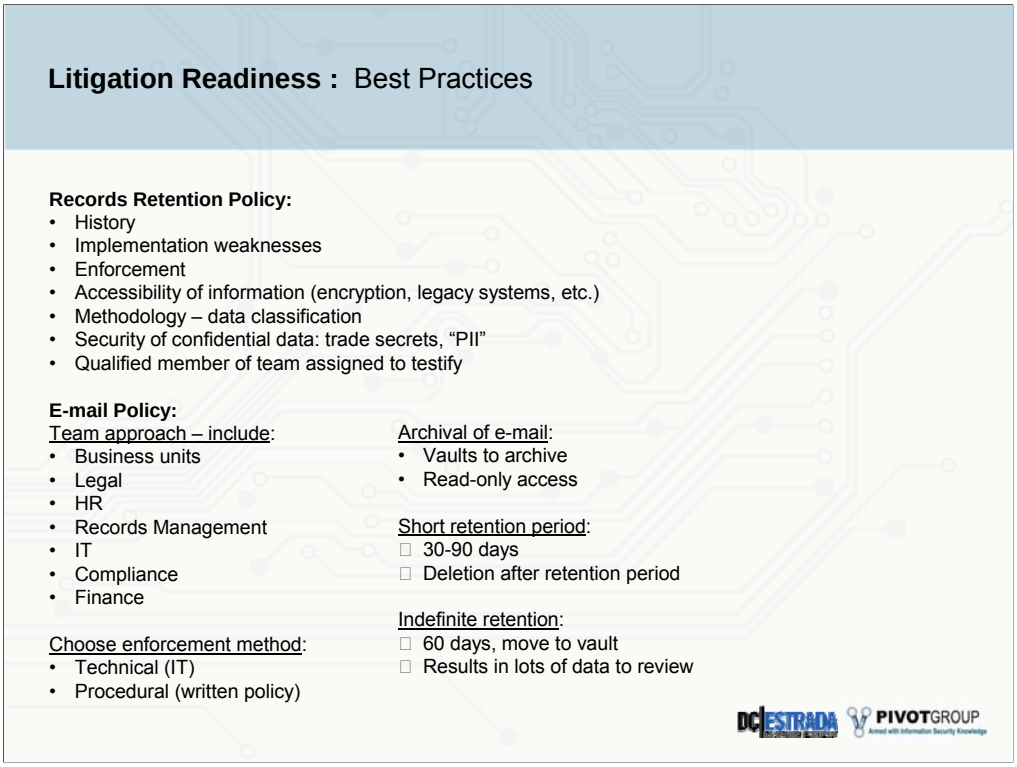
Disposal rules include use of wiping utilities – a hammer is an inexpensive way to dispose of information.

IRS Circular 230 – only applies if attorneys practicing before the IRS

European Union Directive on Data Protection – must be careful when responding to lawsuit that you don't violate this directive by collecting evidence from European Union divisions of the company.

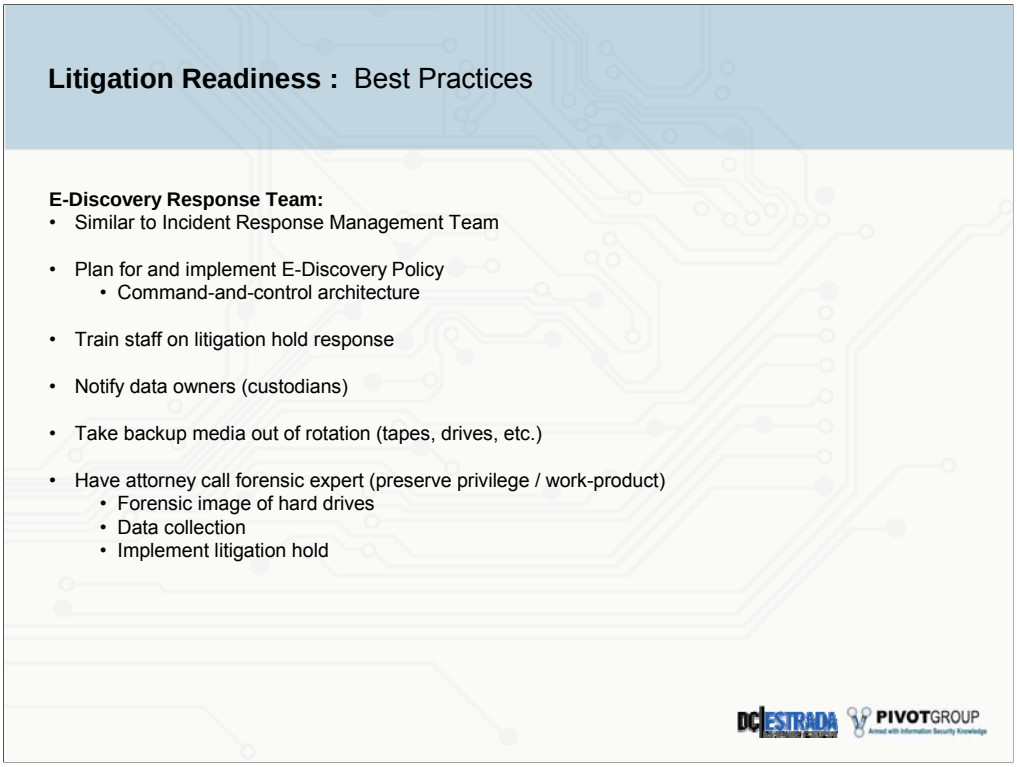
State security breach notification laws – Close to 40 states now have this in place.

Notes:© Faith M. Heikkila, Pivot Group



For more information on e-mail policy development, see Allman, T. Y. (Fall 2007), The Sedona Conference Commentary on Email Management: Guidelines for the Selection of Retention Policy, 8 Sedona Conference Journal 239 - 250
http://www.thesedonaconference.org/content/miscFiles/Commentary_on_Email_Management___revised_cover.pdf

Notes:© Faith M. Heikkila, Pivot Group

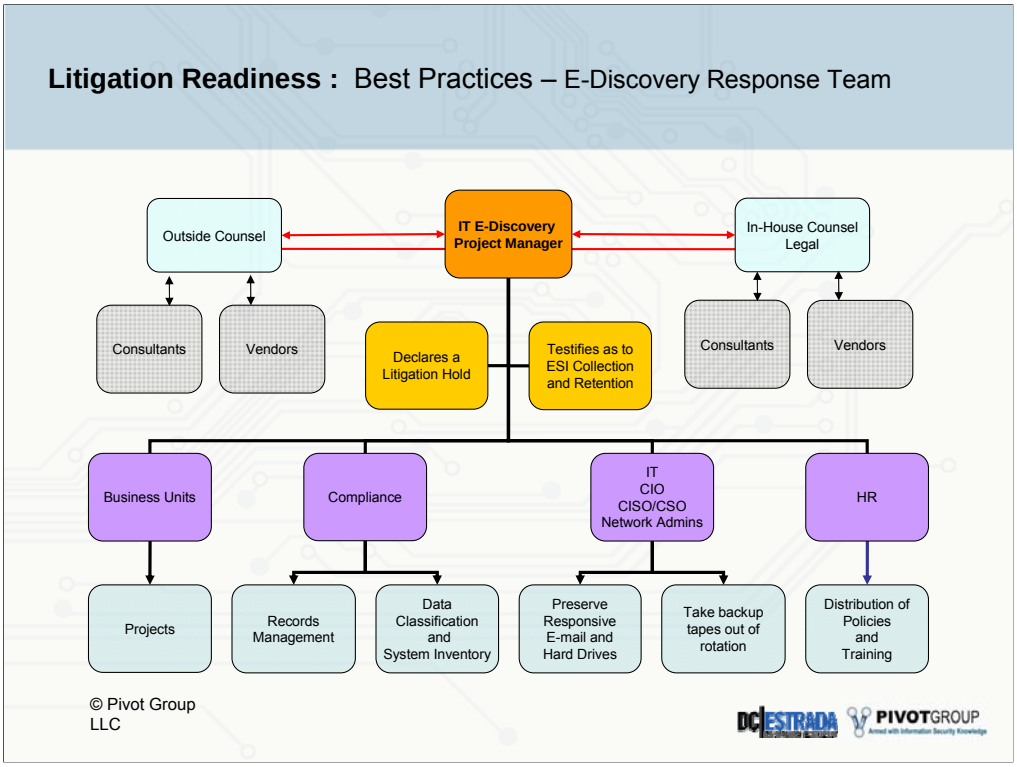


Incident Response –

1. Stop incident by unplugging computer from network
2. Contain incidents by closing off Internet access
3. Recover from incident – repair or patch the virus or issue (i.e., removal of virus from systems)
4. Investigate incident – how did it happen and how can we stop it from happening in the future
5. Remediation – have consultants lined up ahead of time

The E-Discovery Response Team is similar to Incident Response Management Team, wherein they are in charge of stopping the deletion of responsive ESI and protecting the confidentiality, integrity, and availability of ESI containing the business secrets from inadvertent disclosure.

Notes:© Faith M. Heikkila, Pivot Group



The E-Discovery Response Team should comprise various business units or departments of the company.

The development of this team should be tailored to the type of business and include as many diverse groups as possible.

Once the IT E-Discovery Project Manager declares a legal hold, each member of the E-Discovery Response Team should immediately know what to do and begin preserving the responsive ESI.

An E-Discovery Response Team should be created in order to facilitate the legal holds for a company.

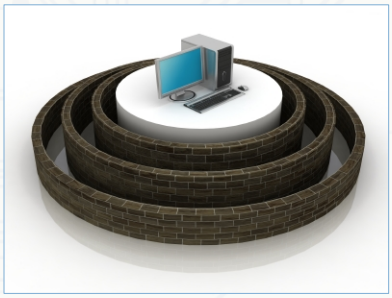
As depicted in the chart, the e-discovery team should designate an E-Discovery Project Manager, who is responsible for declaring a legal hold under the direction of the outside counsel, or if the company has a legal department, the in-house counsel.

Notes:© Faith M. Heikkila, Pivot Group

Litigation Readiness : Best Practices – Data Security

IT security is *very* relevant in readiness:

- Establish rules for security
- Sensitive documents must be protected
- Protective order
  - Discloses how documents are handled
  - Destruction of produced ESI after case
- Third-party security
  - Vendors and experts
  - Opposing party
  - Includes backup and recovery
  - Contractual obligations



DC ESTRADA PIVOTGROUP

The security of the ESI during transit, while in the possession of third parties, such as attorneys and Application Service Providers (ASPs), must be included in the company's e-discovery policy and document management program.

Notes:© Faith M. Heikkila, Pivot Group

E-Discovery Resources :

Amended Federal Rules of Civil Procedure (with Notes):
http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf

2008 E-Discovery Reference Guide
Guidelines, best practices, and technology glossary

D.C. Estrada Information Technology
E-discovery, data forensics, and litigation support

Pivot Group
Tailored information security solutions, e-discovery, document identification and location

Pivot Group Whitepapers:
http://www.pivotgroup.net/whitepapers.html

Useful E-Discovery Web Sites
See printed list, attached to presentation

E-Discovery and Litigation Preparedness Workshop:
May 14, 2008
Location TBD
Reserve your seat today!

Notes:© Faith M. Heikkila, Pivot Group

Contact Information :

DC ESTRADA INFORMATION TECHNOLOGY

www.dcestrada.com

Daniel Estrada
President

1325 Dunham Street SE, Suite 201
Grand Rapids, Michigan 49503

Office: (616) 855-1746
Cell: (616) 856-9633
daniel@dcestrada.com

PIVOTGROUP
Armed with Information Security Knowledge

www.pivotgroup.net

Faith M. Heikkila
Regional Security Services Manager – Great Lakes

5955 West Main
Kalamazoo, Michigan 49009

Office: (269) 544-0030
Cell: (616) 430-8056
fheikkila@pivotgroup.net

Notes:© Faith M. Heikkila, Pivot Group