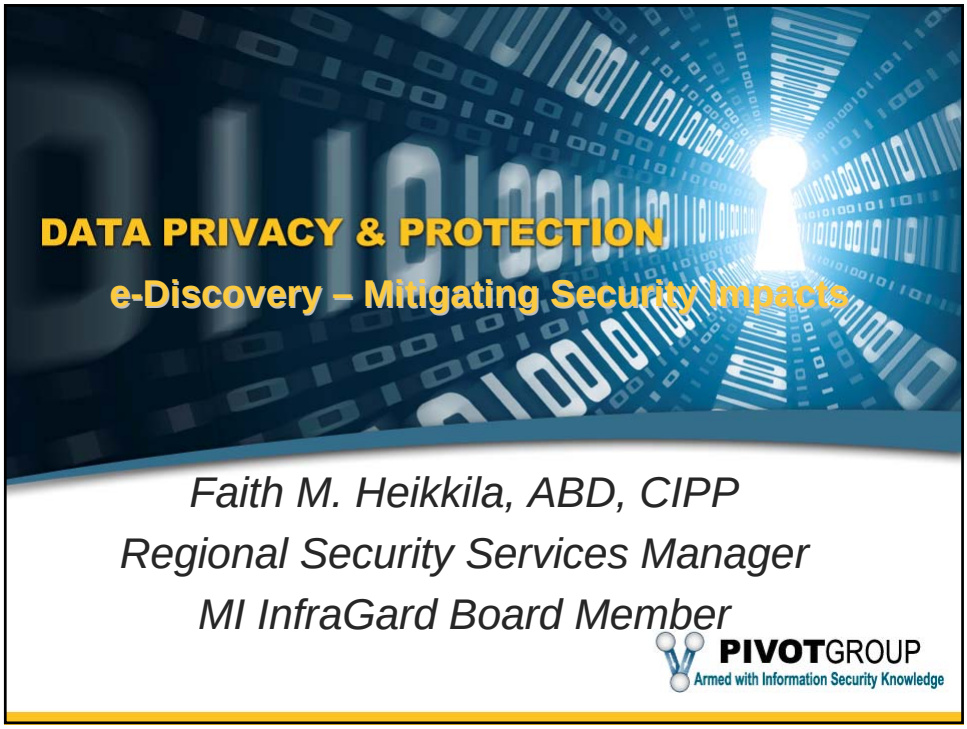


Credentials

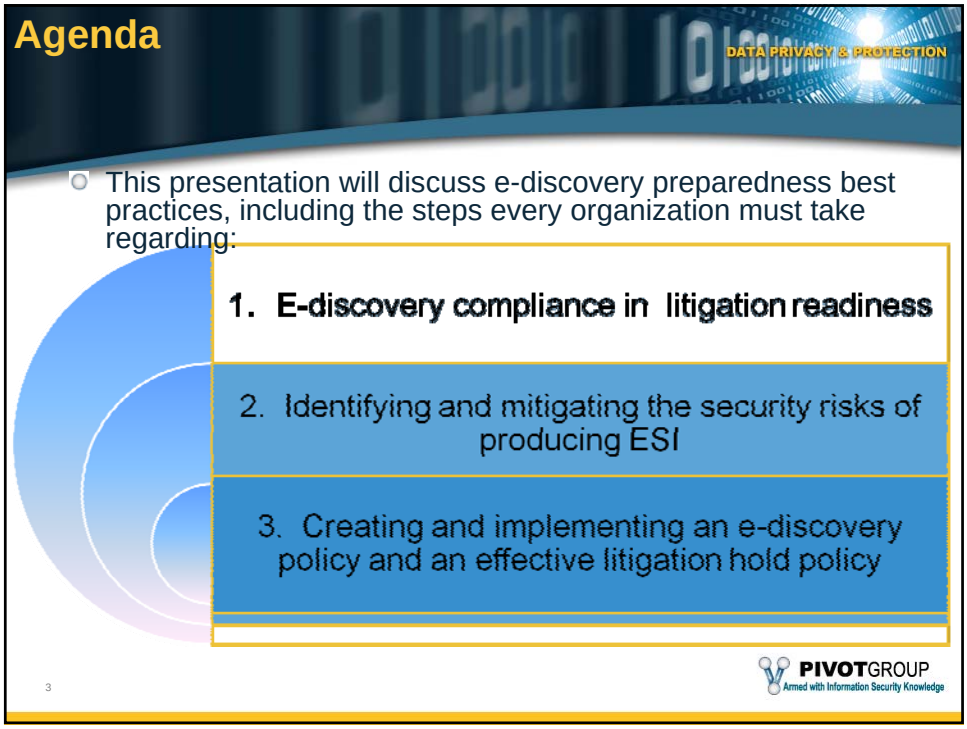
DATA PRIVACY & PROTECTION

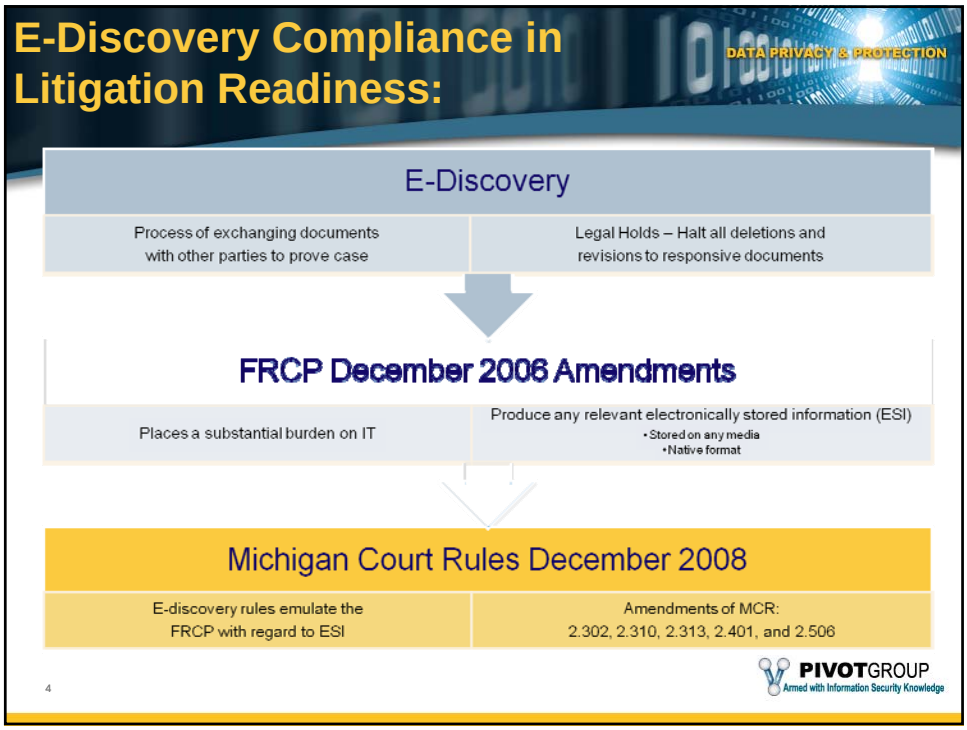
- Information security consultant – Pivot Group
- Michigan InfraGard Board Member
- ConnecTech Greater Kalamazoo Board Member
- Michigan Critical Infrastructure Protection
- Certified Information Privacy Professional (CIPP)
- Previous Work Experience:
  - Complex Litigation Paralegal for 16 years
  - Law firm IT Project Manager for 2 years
  - CIS Chairperson and Assistant Professor for 5 years
- *PhD Candidate in Information Systems, specializing in information assurance at Nova Southeastern University*
- Published and presented a number of articles on security and e-discovery

I am not a lawyer and I do not even play one on TV.
This presentation is: merely my opinion and does not constitute legal advice.
Please contact your attorney for legal advice relevant to your e-discovery needs.

2

PIVOTGROUP
Armed with Information Security Knowledge


Agenda
DATA PRIVACY & PROTECTION
This presentation will discuss e-discovery preparedness best practices, including the steps every organization must take regarding:
1. E-discovery compliance in litigation readiness
2. Identifying and mitigating the security risks of producing ESI
3. Creating and implementing an e-discovery policy and an effective litigation hold policy
3
PIVOTGROUP
Armed with Information Security Knowledge


E-Discovery Compliance in Litigation Readiness:
DATA PRIVACY & PROTECTION
E-Discovery
Process of exchanging documents with other parties to prove case
Legal Holds – Halt all deletions and revisions to responsive documents
FRCP December 2006 Amendments
Places a substantial burden on IT
Produce any relevant electronically stored information (ESI)
•Stored on any media
•Native format
Michigan Court Rules December 2008
E-discovery rules emulate the FRCP with regard to ESI
Amendments of MCR: 2.302, 2.310, 2.313, 2.401, and 2.506
4
PIVOTGROUP
Armed with Information Security Knowledge

E-Discovery Compliance in Litigation Readiness:

DATA PRIVACY & PROTECTION

Contextual Differences

Federal Court Rules	State Court Rules
Envision court-supervised discovery	Envision party-led discovery
Discovery does not begin until court endorses a plan	Court is a passive agent until a disagreement arises
The court is often looking over the parties' shoulders every step of the way	Parties may need to work harder to try to resolve e-discovery issues on their own.
"Must"	"May"

PIVOTGROUP
Armed with Information Security Knowledge

E-Discovery Compliance in Litigation Readiness:

DATA PRIVACY & PROTECTION

Regulatory Compliance
- Courts look for "good faith" effort
  - In almost every e-discovery case
  - Sometimes *more* important than ability to produce

Data Security Breach Notification Laws
- *44 states plus the District of Columbia, Puerto Rico, and the Virgin Islands*
- **Michigan** – Effective July 2, 2007:
  - Includes units of state governmental agencies
  - Excludes courts (circuit, probate, district, or municipal)
  - Health insurance ID number, tax ID, driver license, financial, passport number, etc.
  - Civil fine of $250 for each failure to provide notice with a maximum of $750,000 per breach

Other Applicable Laws
- *PCI* – Must protect credit card numbers – Mask PAN (*primary account number*) when displayed
  - First six and last four digits are the maximum number of digits to be displayed
- HIPAA
  - Security controls, how long retain data, and destruction procedures.
  - Privacy of medical information
- 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.

6

PIVOTGROUP
Armed with Information Security Knowledge

E-Discovery Risks And Dangers:

DATA PRIVACY & PROTECTION

- Time spent on legal holds
- Time spent locating / identifying responsive ESI
- Third-party costs:
  - outside counsel
  - tools
  - experts

High cost and burden to the organization

"Smoking gun" Greatest Challenge Own and Opposing Party's

Inadvertent waiver of privilege / release of secrets or work product

Inability to produce responsive ESI (possible sanctions)

- Metadata
- Bad publicity (skeletons released)
  - Don't be the next "poster child"
- Related challenges: privilege may not exist

- Legacy systems and backups – not retrievable

- Example: ***Scott v. Beth Israel Medical Center***

7

PIVOTGROUP
Armed with Information Security Knowledge

E-Discovery Risks And Dangers:

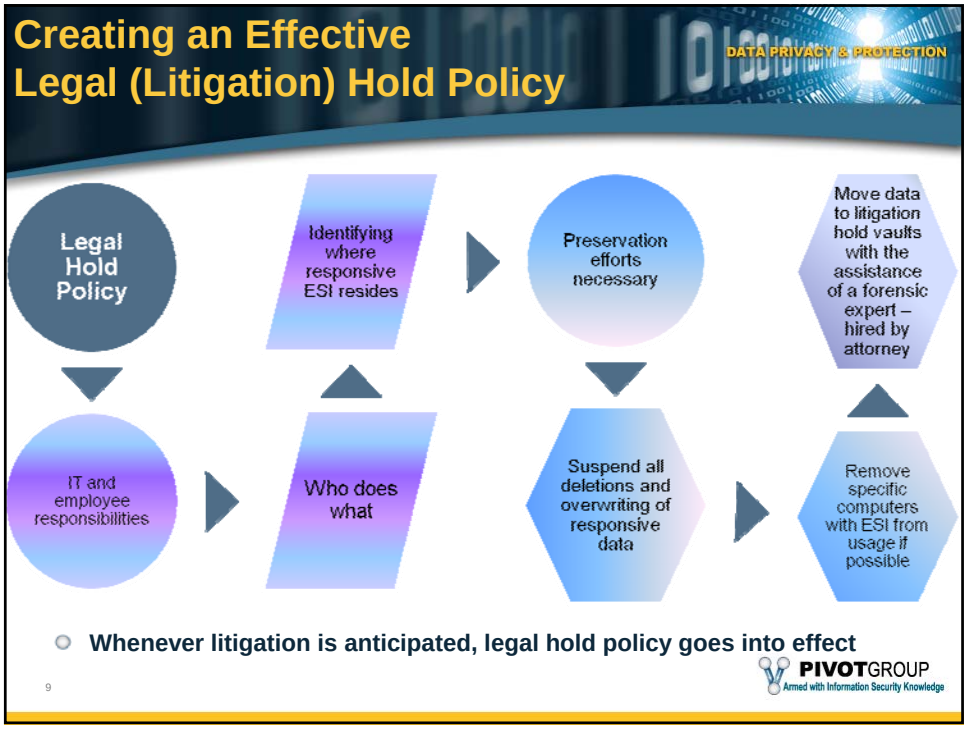
DATA PRIVACY & PROTECTION

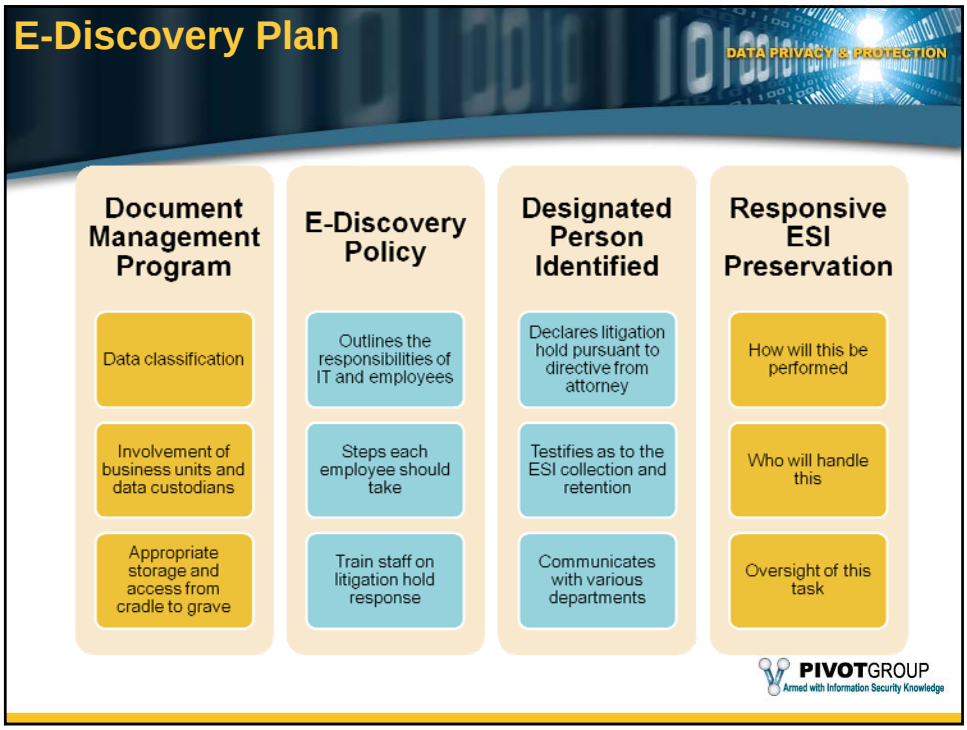
- **Protect against Inadvertent Disclosure during Production**
  - Sensitive intellectual property
  - Personally Identifiable Information (PII)
  - Credit card information
  - Medical information

- **Vendor Management of Third Parties**
  - Web Portals used by litigation support companies and attorneys
  - Security of third party personnel
  - Security clearance background checks
  - Security of data while in control of third parties
    - Authentication of data – unchanged while in hands of third party
    - Last vulnerability assessment results
    - Secure transmission of data
    - Incident response plan of third party
  - Disposal methods

8

PIVOTGROUP
Armed with Information Security Knowledge


Creating an Effective
Legal (Litigation) Hold Policy
DATA PRIVACY & PROTECTION
Legal Hold Policy
Identifying where responsive ESI resides
Preservation efforts necessary
Move data to litigation hold vaults with the assistance of a forensic expert – hired by attorney
IT and employee responsibilities
Who does what
Suspend all deletions and overwriting of responsive data
Remove specific computers with ESI from usage if possible
Whenever litigation is anticipated, legal hold policy goes into effect
PIVOTGROUP
Armed with Information Security Knowledge
9


E-Discovery Plan
DATA PRIVACY & PROTECTION
Document Management Program
Data classification
Involvement of business units and data custodians
Appropriate storage and access from cradle to grave
E-Discovery Policy
Outlines the responsibilities of IT and employees
Steps each employee should take
Train staff on litigation hold response
Designated Person Identified
Declares litigation hold pursuant to directive from attorney
Testifies as to the ESI collection and retention
Communicates with various departments
Responsive ESI Preservation
How will this be performed
Who will handle this
Oversight of this task
PIVOTGROUP
Armed with Information Security Knowledge

E-Discovery Plan

DATA PRIVACY & PROTECTION

Develop an E-Discovery Response Team	E-Discovery Response Team	Train Employees	Attorney Calls Forensic Expert
Acts under legal counsel's direction	Plan for and implement E-Discovery Policy - Command-and-control architecture	Role in preserving ESI	Preserve privilege / work-product
Business Units within organization	Train staff on litigation hold response	Failure to safeguard ESI results in	Forensic image of hard drives
Consultants and vendors in place to assist with collection and preservation efforts	Notify data owners (custodians)	Destruction of evidence (spoliation)	Data collection
	Take backup media out of rotation (tapes, drives, etc.)	Sanctions and monetary judgments	Implement litigation hold

11

PIVOTGROUP
Armed with Information Security Knowledge

Litigation Readiness: Best Practices – Mitigating Security Impacts

DATA PRIVACY & PROTECTION

IT security is *very* relevant in readiness:
- Establish rules for security
- Sensitive documents must be protected
- E-discovery policies and document management
- Litigation hold policy

Protective order
- Discloses how documents are handled
- Outline PII production safeguards
- Inadvertent disclosure of PII
- Destruction of produced ESI after case

Third-party security
- Vendors and experts
- Opposing party
- Includes backup and recovery
- Contractual obligations

Programs and Assessments
- Information Security Management System Program
- Risk Assessments
- Vendor Management Program
- Data Privacy and Protection Programs

13

PIVOTGROUP
Armed with Information Security Knowledge

E-Discovery Resources

DATA PRIVACY & PROTECTION

- **E-Discovery: Identifying and Mitigating Security Risks during Litigation**, *IT Professional*, July/August 2008, p. 20-25 http://www.pivotgroup.net/whitepapers.html
- Amended Federal Rules of Civil Procedure (with Notes): **http://www.uscourts.gov/rules/EDiscovery_w_Notes.pdf**
- MI Court Rules : **http://coa.courts.mi.gov/rules/**
- **The Sedona Conference**
  http://www.thesedonaconference.org/

14

PIVOTGROUP
Armed with Information Security Knowledge

Contact Information

DATA PRIVACY & PROTECTION

- **Faith M. Heikkila**
  Pivot Group, LLC
  Regional Security Services Manager – Great Lakes
  5955 West Main
  Kalamazoo, Michigan 49009
- Office: (269) 544-0030
- Cell: (616) 430-8056
- fheikkila@pivotgroup.net

15

PIVOTGROUP
Armed with Information Security Knowledge