Citation Key

for more information see: http://open.umich.edu/wiki/CitationPolicy

Use + Share + Adapt

{ Content the copyright holder, author, or law permits you to use, share and adapt. }

Public Domain – Government: Works that are produced by the U.S. Government. (USC 17 § 105)

Public Domain – Expired: Works that are no longer protected due to an expired copyright term.

Public Domain – Self Dedicated: Works that a copyright holder has dedicated to the public domain.

Creative Commons – Zero Waiver

Creative Commons – Attribution License

Creative Commons – Attribution Share Alike License

Creative Commons – Attribution Noncommercial License

Creative Commons – Attribution Noncommercial Share Alike License

GNU – Free Documentation License

Make Your Own Assessment

{ Content Open.Michigan believes can be used, shared, and adapted because it is ineligible for copyright. }

Public Domain – Ineligible: Works that are ineligible for copyright protection in the U.S. (USC 17 § 102(b)) *laws in your jurisdiction may differ

{ Content Open.Michigan has used under a Fair Use determination. }

Fair Use: Use of works that is determined to be Fair consistent with the U.S. Copyright Act. (USC 17 § 107) *laws in your jurisdiction may differ

Our determination **DOES NOT** mean that all uses of this 3rd-party content are Fair Uses and we **DO NOT** guarantee that your use of the content is Fair.

To use this content you should **do your own independent analysis** to determine whether or not your use will be Fair.

Data Security Enforcement

510 - Data Security and Privacy: Legal, Policy, and Enterprise Issues
University of Michigan School of Information
Week 6

Law Enforcement

Vary with Jurisdiction

- Civil
  - Court
  - Administrative
- Criminal
- Federal
- State

Vary with Context

- Formal investigation
  - Voluntary response
  - Mandatory response
- Target or third party
- “Just between you, me, and the lamp post….”
  - Procedural assistance
  - Investigation assistance
  - General information

Law Enforcement Action Basics

- Laws vary
- Regulations vary
- Policies vary
- Procedures vary
- Individuals vary
- Necessary tactics vary
- However….

Fundamental Rules

- The fundamental points do not vary
- Show respect
- Don’t play games

Federal Trade Commission

- Civil jurisdiction only
  - Different burden of proof
- Section 5 actions
  - Penalties are injunction or consumer redress
- Authorizing statute cases; *e.g.,* GLB
  - Fines/violation
- Can bring case using more than one

Usual Beginning

- Relatively informal
- Access letter or similar document
  - AKA Voluntary process
- “We have opened a law enforcement investigation. Please provide documents responsive to the following questions….”

“Documents” Will Be Broad

- The term "documents" means all written, recorded, and graphic materials and all electronic data of every kind in the possession, custody or control of the company, whether on or off company premises….The term "documents" includes electronic mail or correspondence, drafts of documents, metadata, embedded, hidden and other bibliographic or historical data describing or relating to documents created, revised, or distributed on computer systems. . . . Therefore, the company shall produce documents that exist in electronic form, including data stored in personal computers, portable computers, workstations, minicomputers, cellular telephones, electronic messaging devices, pagers, personal digital assistants, archival voice storage systems, group and collaborative tools, portable or removable storage media, mainframes, servers, backup disks and tapes, archive disks and tapes, and other forms of online or offline storage….

Access Letter

- Not wise to ignore
- Assign best possible person in company for each question
- Check if outside contractor might already have answers or be helpful in examining
- Find out what documents are where and in what form
- Contact requesting attorney to discuss any issues concerning terms of letter

After Review

- Document submission
- Frequently face to face meeting
  - Company officials
  - Attorneys
  - Experts

Results

- May resolve issues with no further action
- Lessens burdens if must proceed farther
- Can set atmosphere if must proceed farther

Civil Action – Mandatory

- Civil investigative demand (CID)
  - AKA compulsory process
- "We have opened a law enforcement investigation. Please provide documents… responsive to the following questions…."
- Signed by commissioner

Process Differences

- Compulsory not limited to documents
  - Interrogatory – provide written answers to questions
  - Deposition – provide someone to testify under oath
- **DON'T IGNORE**
  - Can be contempt sanctions for non-compliance

Results

- Negotiated consent order
  - Issued with complaint
  - Put on public record for comment
  - Can happen at any time
- Complaint without consent order
  - Starts the road to trial
- Close investigation
  - Issue closing letter

Extreme Results

- Failure to comply with consent terms
  - New consent with stiffer terms
  - Civil contempt
  - Criminal contempt

Be Proactive with LE

- Self interest - perception is important
- Provide guidance/assistance that may lessen respective burdens
- Publicize security activities
- Build relationship over time
  - Meetings, conventions
- LE more accessible and receptive if you have problems
- You know LE organization and organization knows you

Security Programs

Security Plan Norms

- Must be consistent with
  - Business operations
  - Legal compliance framework
  - Management goals
  - Organizational culture
  - Systems architecture

Security Plan Organization

- Boards of Directors
- Senior management
- Internal management
- Operational staff

Internal Management

- Business unit managers
- HR
- Legal
- Financial
- Technical
- Security
- PR

Assessment

- Includes Gap Analysis
- Analyze environment and assess risks and vulnerabilities
- Assess potential for problem
- Identify solutions or countermeasures
  - Appropriate and cost effective safeguards

Risk Assessment Strategies

- Avoid
- Mitigate
- Accept
- Transfer/Insure

IT Risk Managers

- Comparatively new concept
- Core of any approach, even if term not used
- Often taken from financial auditors and analysts

Common Flaws

- Failure to focus on value of information and business reputation
- Fix as little as possible and not follow up
- Assign untrained people and not give them instruction
- Ignoring problems
- Using surface solutions

Change Management

- Another relatively new concept
- Can help with many problems
- Systematic way to introduce and manage change
- Procedures for introducing and implementing
- Audit trail to trace problems back

Classification

- Gives framework for setting risk priorities
- Seems straightforward
  - Can be complicated
  - Often not done in systematic way
- Flexible process
- Must examine data life cycle
  - Create, access, use, modify, store
- Similar approach for applications and systems

Policies

- Components of plan
- Frameworks for decisions
- Place to add standards, guidelines, best practices
- Four levels
  - Corporate
  - Functional
  - Computing
  - Security baseline

Procedures

- Put into effect

Review

- At least annually for:
  - Effectiveness
  - Compliance
  - Vulnerability