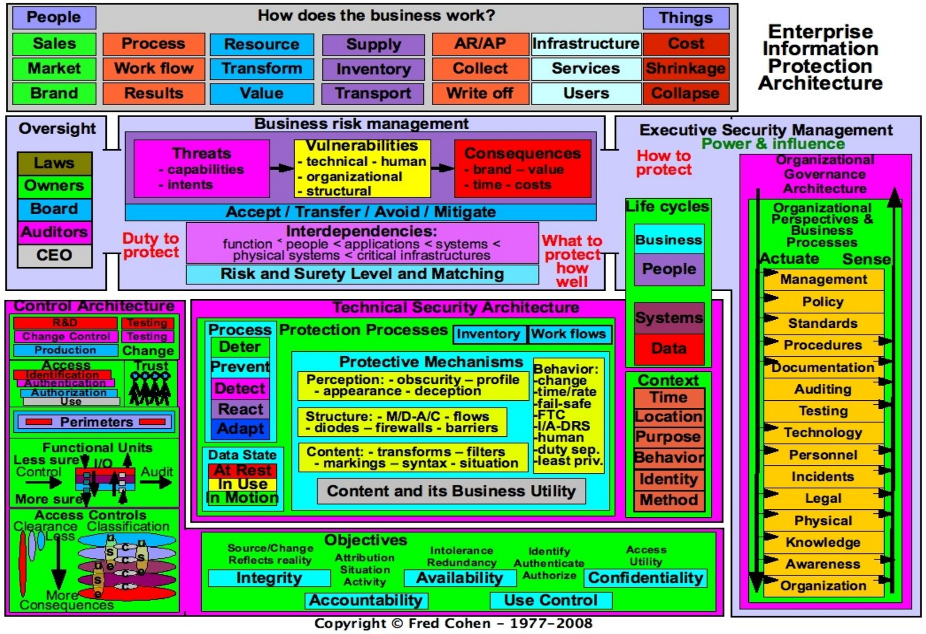
Keynote

Where do enterprise protection and digital forensics converge? AND Where do they diverge?

Computer Forensics Show – Nov 1, 2010

Dr. Fred Cohen
President - California Sciences Institute
CEO – Fred Cohen & Associates

Outline



People
How does the business work?
Things
Sales | Process | Resource | Supply | AR/AP | Infrastructure | Cost
Market | Work flow | Transform | Inventory | Collect | Services | Shrinkage
Brand | Results | Value | Transport | Write off | Users | Collapse

Enterprise Information Protection Architecture

Oversight
Laws
Owners
Board
Auditors
CEO

Business risk management
Threats - capabilities - intents
Vulnerabilities - technical - human - organizational - structural
Consequences - brand – value - time - costs
Accept / Transfer / Avoid / Mitigate
Duty to protect
Interdependencies: function < people < applications < systems < physical systems < critical infrastructures
Risk and Surety Level and Matching
What to protect how well

Executive Security Management
Power & influence
How to protect
Life cycles
Business
People
Systems
Data
Context
Time
Location
Purpose
Behavior
Identity
Method

Organizational Governance Architecture
Organizational Perspectives & Business Processes
Actuate
Sense
Management
Policy
Standards
Procedures
Documentation
Auditing
Testing
Technology
Personnel
Incidents
Legal
Physical
Knowledge
Awareness
Organization

Control Architecture
R&D | Testing
Change Control | Testing
Production | Change
Access
Identification
Authentication
Authorization
Use
Trust
Perimeters
Functional Units
Less sure
I/O
Control
Audit
More sure
Access Controls
Clearance
Classification
Less
More
Consequences

Technical Security Architecture
Process
Deter
Prevent
Detect
React
Adapt
Protection Processes
Inventory
Work flows
Protective Mechanisms
Perception: - obscurity – profile - appearance - deception
Structure: - M/D-A/C - flows - diodes – firewalls - barriers
Content: - transforms – filters - markings – syntax - situation
Behavior: -change -time/rate -fail-safe -FTC -I/A-DRS -human -duty sep. -least priv.
Data State
At Rest
In Use
In Motion
Content and its Business Utility

Objectives
Source/Change Reflects reality
Integrity
Attribution Situation Activity
Intolerance Redundancy
Availability
Identify Authenticate Authorize
Access Utility
Confidentiality
Accountability
Use Control

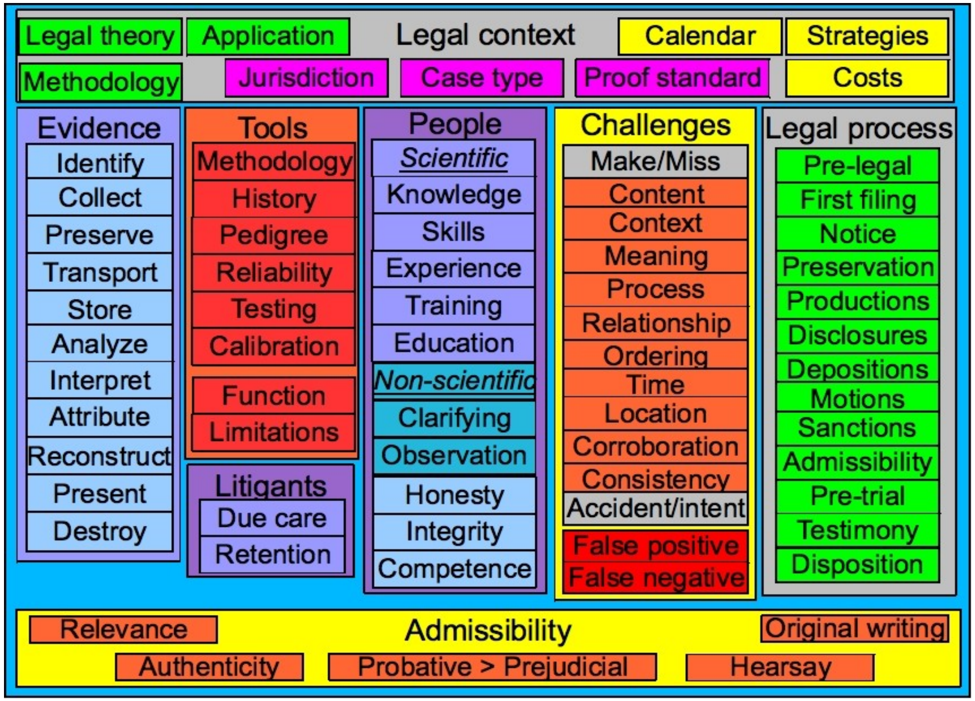
Copyright © Fred Cohen - 1977-2008

<<<------------------

- Enterprise protection:
  - Assure utility of content
    - To management specified tolerance

- Digital forensics:
  - What happened?
  - To an appropriate legal standard!

------------------->>>



Legal theory | Application | Legal context | Calendar | Strategies
Methodology | Jurisdiction | Case type | Proof standard | Costs

Evidence
Identify
Collect
Preserve
Transport
Store
Analyze
Interpret
Attribute
Reconstruct
Present
Destroy

Tools
Methodology
History
Pedigree
Reliability
Testing
Calibration
Function
Limitations

Litigants
Due care
Retention

People
Scientific
Knowledge
Skills
Experience
Training
Education
Non-scientific
Clarifying
Observation
Honesty
Integrity
Competence

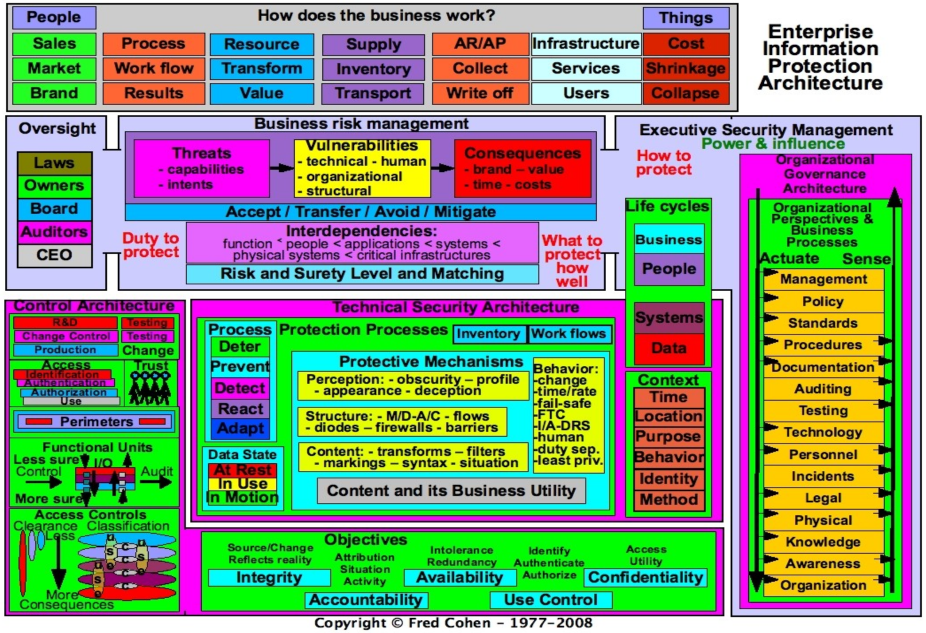
Challenges
Make/Miss
Content
Context
Meaning
Process
Relationship
Ordering
Time
Location
Corroboration
Consistency
Accident/intent
False positive
False negative

Legal process
Pre-legal
First filing
Notice
Preservation
Productions
Disclosures
Depositions
Motions
Sanctions
Admissibility
Pre-trial
Testimony
Disposition

Relevance | Admissibility | Original writing
Authenticity | Probative > Prejudicial | Hearsay

California Sciences Institute

Who's here?


Enterprise Information Protection Architecture

How does the business work?
People | Things
Sales | Market | Brand
Process | Work flow | Results
Resource | Transform | Value
Supply | Inventory | Transport
AR/AP | Collect | Write off
Infrastructure | Services | Users
Cost | Shrinkage | Collapse

Oversight: Laws | Owners | Board | Auditors | CEO

Business risk management
Threats - capabilities - intents → Vulnerabilities - technical - human - organizational - structural → Consequences - brand – value - time - costs
Accept / Transfer / Avoid / Mitigate
Duty to protect
Interdependencies: function < people < applications < systems < physical systems < critical infrastructures
Risk and Surety Level and Matching
What to protect how well

Executive Security Management
Power & influence
How to protect
Organizational Governance Architecture
Organizational Perspectives & Business Processes
Actuate Sense
Management | Policy | Standards | Procedures | Documentation | Auditing | Testing | Technology | Personnel | Incidents | Legal | Physical | Knowledge | Awareness | Organization

Life cycles: Business | People | Systems | Data

Context: Time | Location | Purpose | Behavior | Identity | Method

Control Architecture
R&D | Testing
Change Control | Testing
Production | Change
Access: Identification | Authentication | Authorization | Use
Trust
Perimeters
Functional Units: Less sure | I/O | Control | Audit | More sure
Access Controls: Clearance | Classification | Less | More Consequences

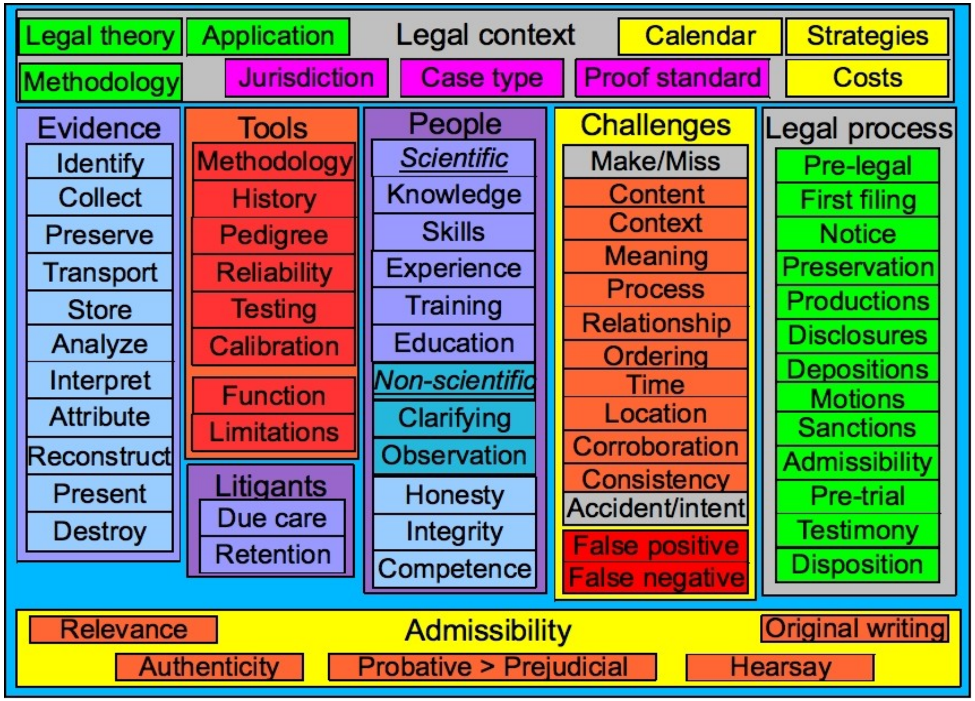
Technical Security Architecture
Process: Deter | Prevent | Detect | React | Adapt
Protection Processes: Inventory | Work flows
Protective Mechanisms
Perception: - obscurity – profile - appearance - deception
Structure: - M/D-A/C - flows - diodes – firewalls - barriers
Content: - transforms – filters - markings – syntax - situation
Behavior: -change -time/rate -fail-safe -FTC -I/A-DRS -human -duty sep. -least priv.
Content and its Business Utility
Data State: At Rest | In Use | In Motion

Objectives
Source/Change Reflects reality | Integrity
Attribution Situation Activity
Intolerance Redundancy | Availability
Identify Authenticate Authorize
Access Utility | Confidentiality
Accountability | Use Control

Copyright © Fred Cohen – 1977–2008

- Chief security officers
- Network security folks
- CISOs
- Experts / researchers

- Law enforcement
- Lawyers and Judges
- Corporate counsel
- Electronic discovery
- Experts / researchers


Legal theory | Application | Legal context | Calendar | Strategies
Methodology | Jurisdiction | Case type | Proof standard | Costs

Evidence: Identify | Collect | Preserve | Transport | Store | Analyze | Interpret | Attribute | Reconstruct | Present | Destroy

Tools: Methodology | History | Pedigree | Reliability | Testing | Calibration | Function | Limitations

Litigants: Due care | Retention

People: *Scientific* | Knowledge | Skills | Experience | Training | Education | *Non-scientific* | Clarifying | Observation | Honesty | Integrity | Competence

Challenges: Make/Miss | Content | Context | Meaning | Process | Relationship | Ordering | Time | Location | Corroboration | Consistency | Accident/intent | False positive | False negative

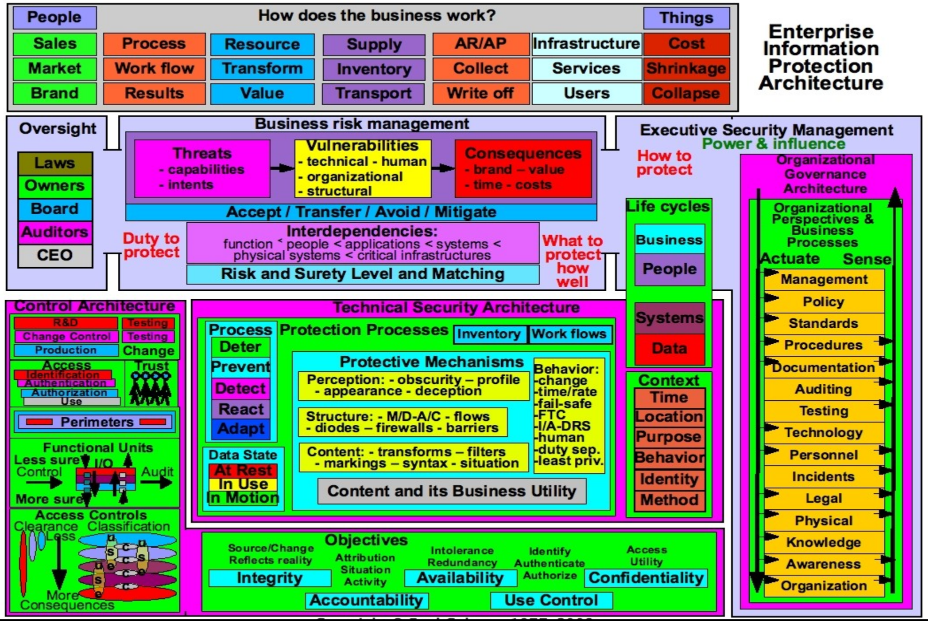
Legal process: Pre-legal | First filing | Notice | Preservation | Productions | Disclosures | Depositions | Motions | Sanctions | Admissibility | Pre-trial | Testimony | Disposition

Relevance | Admissibility | Original writing
Authenticity | Probative > Prejudicial | Hearsay

Your speaker

- CEO - Fred Cohen & Associates / President CalSci
  - Enterprise information protection architecture
  - Digital forensics for (usually high-valued) legal cases
  - 501(c)3 research and educational institution
  - M.S. Advanced Investigation / Ph.D. Digital Forensics
- B.S. EE (C-MU '77), M.S. Info Sci (Pitt '81), Ph.D. EE (USC '86)
- >30 years of information protection R&D, design, engineering, testing, implementation, operation, etc.
- >20 years since first digital forensics case
- POST certified instructor in digital forensics, Guest lecturer FLETC, PMTS Sandia National Labs, etc.
- >>100 peer reviewed publications, many conference talks, …

Outline

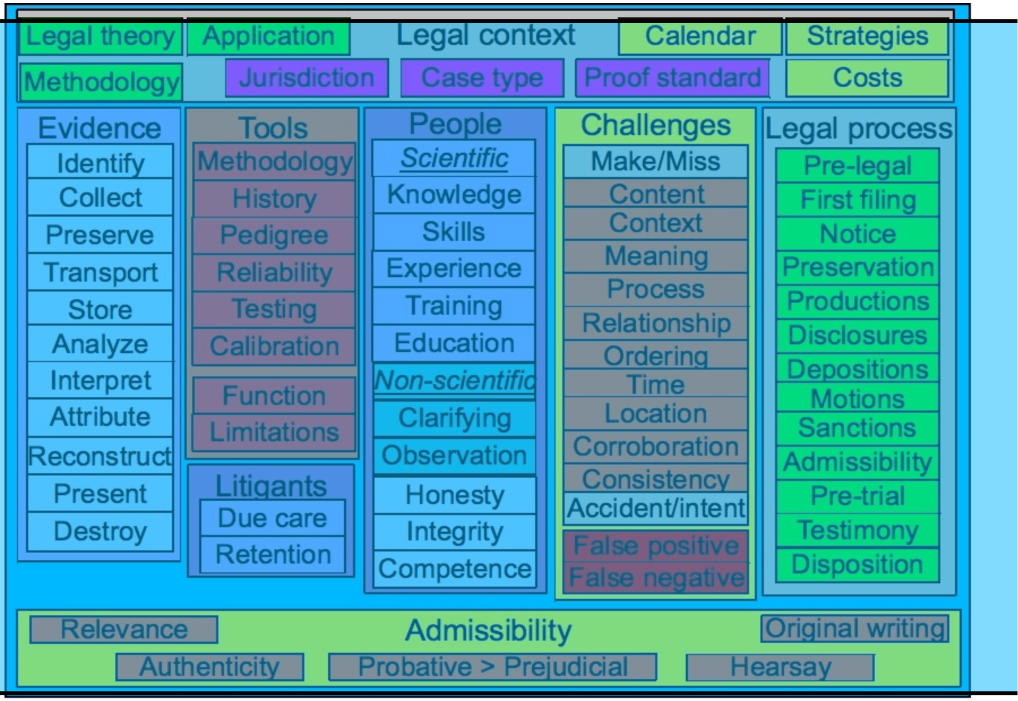


<<<-------------------

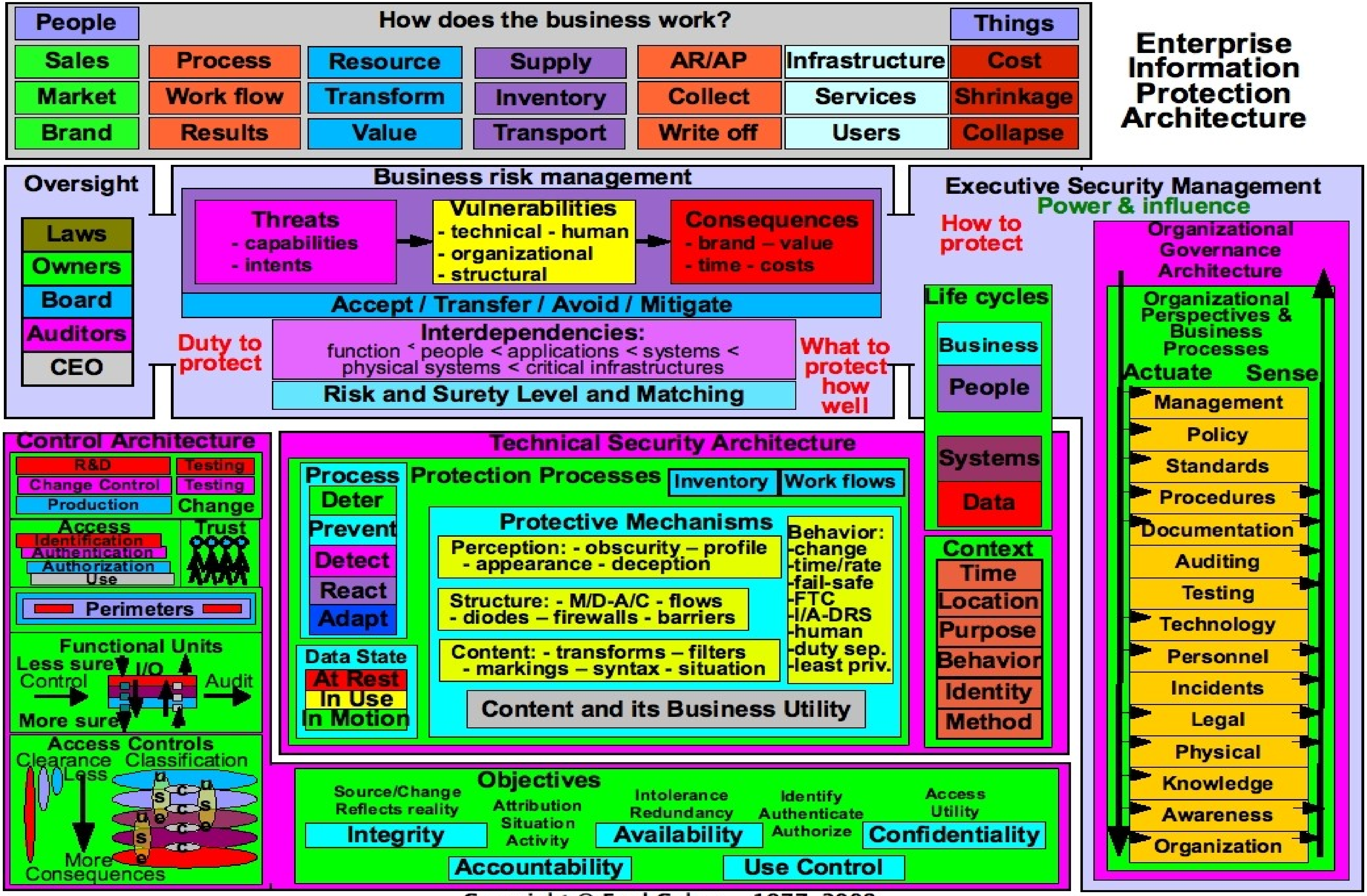
- Enterprise protection:
  - Assure utility of content
    - To management specified tolerance

- Digital forensics:
  - What happened?
  - To an appropriate legal standard!

------------------->>>



Enterprise information protection



Enterprise Information Protection Architecture

How does the business work?

People | Things

Sales, Market, Brand

Process, Work flow, Results

Resource, Transform, Value

Supply, Inventory, Transport

AR/AP, Collect, Write off

Infrastructure, Services, Users

Cost, Shrinkage, Collapse

Oversight

Laws, Owners, Board, Auditors, CEO

Business risk management

Threats
- capabilities
- intents

Vulnerabilities
- technical - human
- organizational
- structural

Consequences
- brand – value
- time - costs

Accept / Transfer / Avoid / Mitigate

Duty to protect

Interdependencies:
function < people < applications < systems < physical systems < critical infrastructures

Risk and Surety Level and Matching

What to protect how well

Executive Security Management

Power & influence

How to protect

Organizational Governance Architecture

Organizational Perspectives & Business Processes

Actuate | Sense

Management, Policy, Standards, Procedures, Documentation, Auditing, Testing, Technology, Personnel, Incidents, Legal, Physical, Knowledge, Awareness, Organization

Life cycles

Business, People, Systems, Data

Context

Time, Location, Purpose, Behavior, Identity, Method

Control Architecture

R&D | Testing

Change Control | Testing

Production | Change

Access: Identification, Authentication, Authorization, Use

Trust

Perimeters

Functional Units

Less sure, Control, I/O, Audit, More sure

Access Controls

Clearance, Classification

Less, More Consequences

u s e, c

Technical Security Architecture

Process: Deter, Prevent, Detect, React, Adapt

Protection Processes

Inventory | Work flows

Protective Mechanisms

Perception: - obscurity – profile - appearance - deception

Structure: - M/D-A/C - flows - diodes – firewalls - barriers

Content: - transforms – filters - markings – syntax - situation

Behavior:
-change
-time/rate
-fail-safe
-FTC
-I/A-DRS
-human
-duty sep.
-least priv.

Content and its Business Utility

Data State: At Rest, In Use, In Motion

Objectives

Source/Change, Reflects reality — Integrity

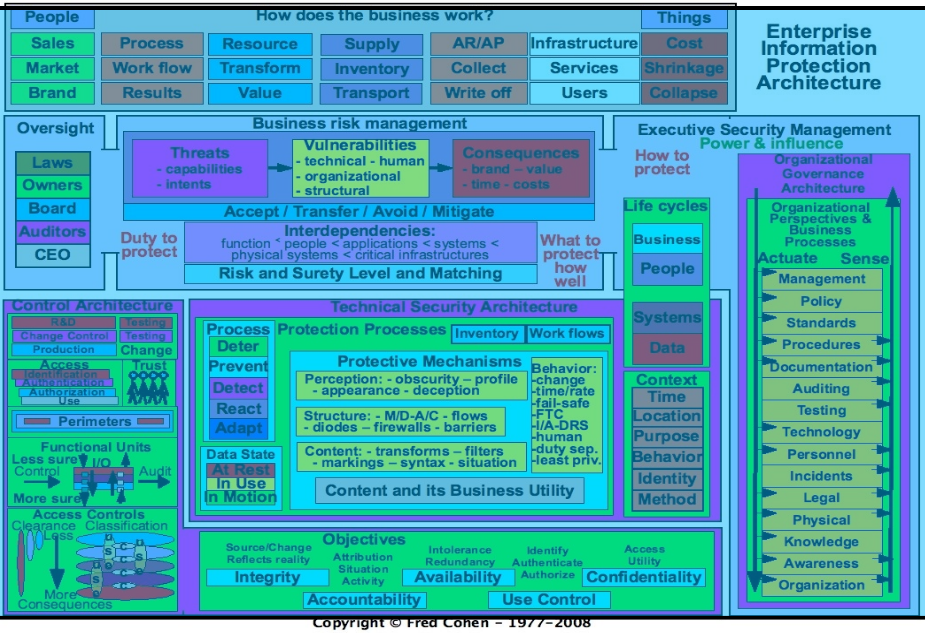
Attribution, Situation, Activity — Accountability

Intolerance, Redundancy — Availability

Identify, Authenticate, Authorize — Use Control

Access, Utility — Confidentiality

Outline



People
How does the business work?
Things
Sales | Process | Resource | Supply | AR/AP | Infrastructure | Cost
Market | Work flow | Transform | Inventory | Collect | Services | Shrinkage
Brand | Results | Value | Transport | Write off | Users | Collapse

Enterprise Information Protection Architecture

Oversight
Laws
Owners
Board
Auditors
CEO

Business risk management
Threats - capabilities - intents
Vulnerabilities - technical - human - organizational - structural
Consequences - brand – value - time - costs
Accept / Transfer / Avoid / Mitigate
Duty to protect
Interdependencies: function < people < applications < systems < physical systems < critical infrastructures
Risk and Surety Level and Matching
What to protect how well

Executive Security Management
Power & influence
How to protect
Organizational Governance Architecture
Life cycles
Business
People
Systems
Data
Organizational Perspectives & Business Processes
Actuate
Sense
Management
Policy
Standards
Procedures
Documentation
Auditing
Testing
Technology
Personnel
Incidents
Legal
Physical
Knowledge
Awareness
Organization

Control Architecture
R&D
Testing
Change Control
Testing
Production
Change
Access
Identification
Authentication
Authorization
Use
Trust
Perimeters
Functional Units
Less sure
I/O
Control
Audit
More sure
Access Controls
Clearance
Classification
Less
More
Consequences

Technical Security Architecture
Process
Deter
Prevent
Detect
React
Adapt
Protection Processes
Inventory
Work flows
Protective Mechanisms
Perception: - obscurity – profile - appearance - deception
Structure: - M/D-A/C - flows - diodes – firewalls - barriers
Content: - transforms – filters - markings – syntax - situation
Behavior: -change -time/rate -fail-safe -FTC -I/A-DRS -human -duty sep. -least priv.
Data State
At Rest
In Use
In Motion
Content and its Business Utility
Context
Time
Location
Purpose
Behavior
Identity
Method

Objectives
Source/Change Reflects reality
Integrity
Attribution Situation Activity
Intolerance Redundancy
Availability
Identify Authenticate Authorize
Access Utility
Confidentiality
Accountability
Use Control

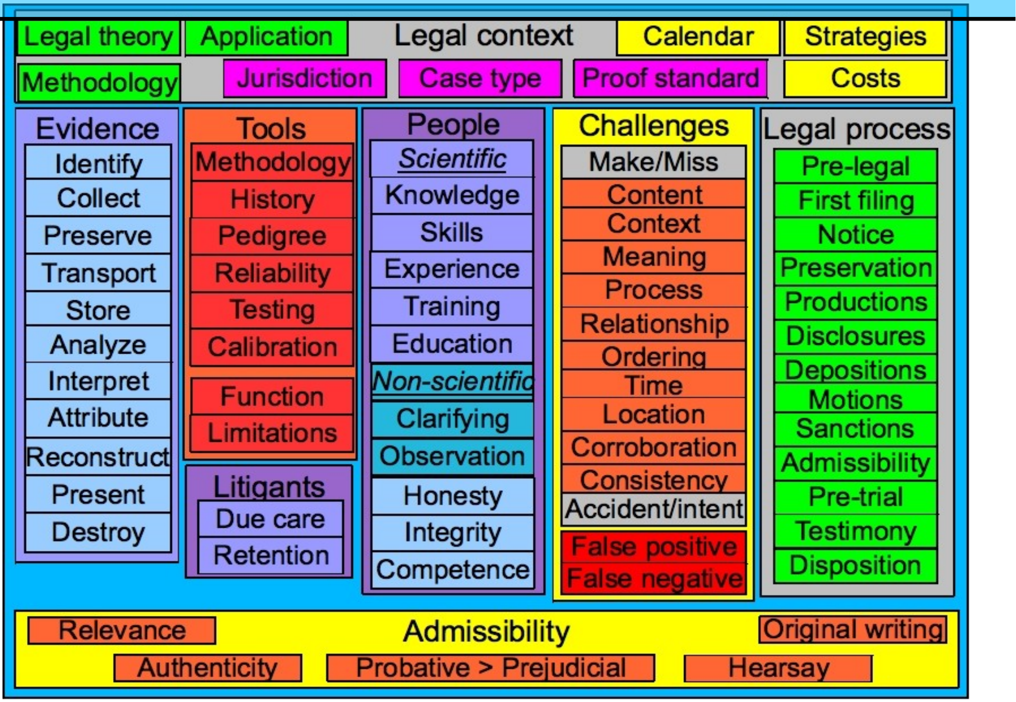
Copyright © Fred Cohen - 1977-2008

<<<------------------

- Enterprise protection:
  - Assure utility of content
  - To management specified tolerance

- Digital forensics:
  - What happened?
  - To an appropriate legal standard!

-------------------->>>



Legal theory
Application
Legal context
Calendar
Strategies
Methodology
Jurisdiction
Case type
Proof standard
Costs

Evidence
Identify
Collect
Preserve
Transport
Store
Analyze
Interpret
Attribute
Reconstruct
Present
Destroy

Tools
Methodology
History
Pedigree
Reliability
Testing
Calibration
Function
Limitations

Litigants
Due care
Retention

People
Scientific
Knowledge
Skills
Experience
Training
Education
Non-scientific
Clarifying
Observation
Honesty
Integrity
Competence

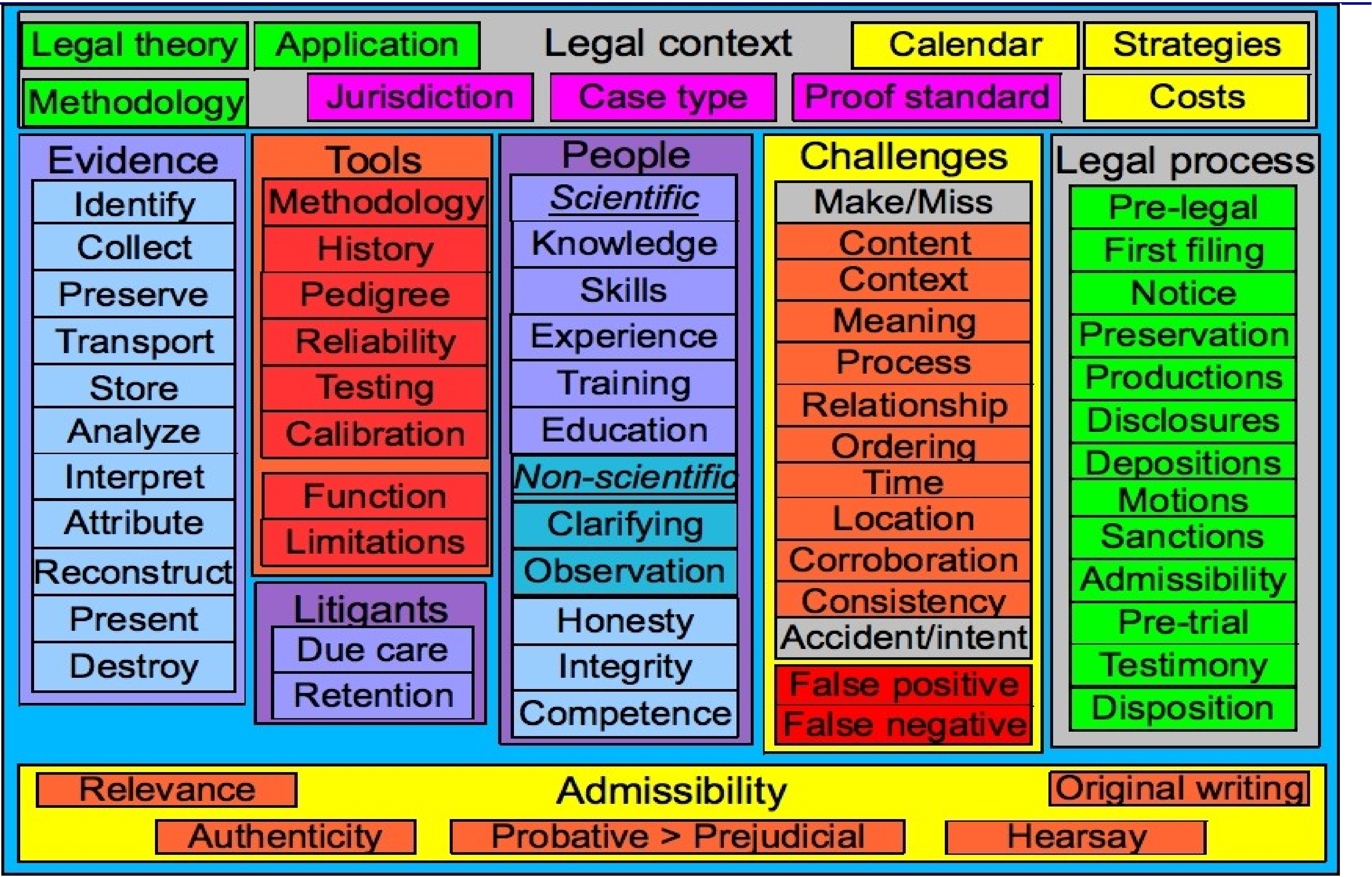
Challenges
Make/Miss
Content
Context
Meaning
Process
Relationship
Ordering
Time
Location
Corroboration
Consistency
Accident/intent
False positive
False negative

Legal process
Pre-legal
First filing
Notice
Preservation
Productions
Disclosures
Depositions
Motions
Sanctions
Admissibility
Pre-trial
Testimony
Disposition

Relevance
Admissibility
Original writing
Authenticity
Probative > Prejudicial
Hearsay

California Sciences Institute

Digital Forensics in Context



Legal context

- Legal theory
- Application
- Methodology
- Jurisdiction
- Case type
- Proof standard
- Calendar
- Strategies
- Costs

Evidence

- Identify
- Collect
- Preserve
- Transport
- Store
- Analyze
- Interpret
- Attribute
- Reconstruct
- Present
- Destroy

Tools

- Methodology
- History
- Pedigree
- Reliability
- Testing
- Calibration
- Function
- Limitations

Litigants

- Due care
- Retention

People

Scientific

- Knowledge
- Skills
- Experience
- Training
- Education

Non-scientific

- Clarifying
- Observation

- Honesty
- Integrity
- Competence

Challenges

- Make/Miss
- Content
- Context
- Meaning
- Process
- Relationship
- Ordering
- Time
- Location
- Corroboration
- Consistency
- Accident/intent
- False positive
- False negative

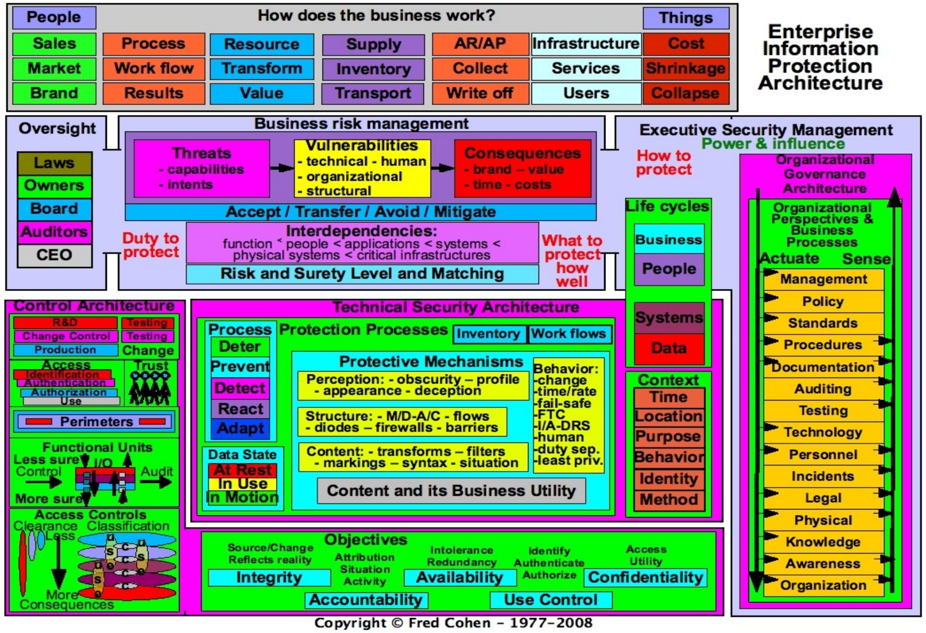
Legal process

- Pre-legal
- First filing
- Notice
- Preservation
- Productions
- Disclosures
- Depositions
- Motions
- Sanctions
- Admissibility
- Pre-trial
- Testimony
- Disposition

Admissibility

- Relevance
- Original writing
- Authenticity
- Probative > Prejudicial
- Hearsay

Outline – Where worlds collide



Enterprise Information Protection Architecture

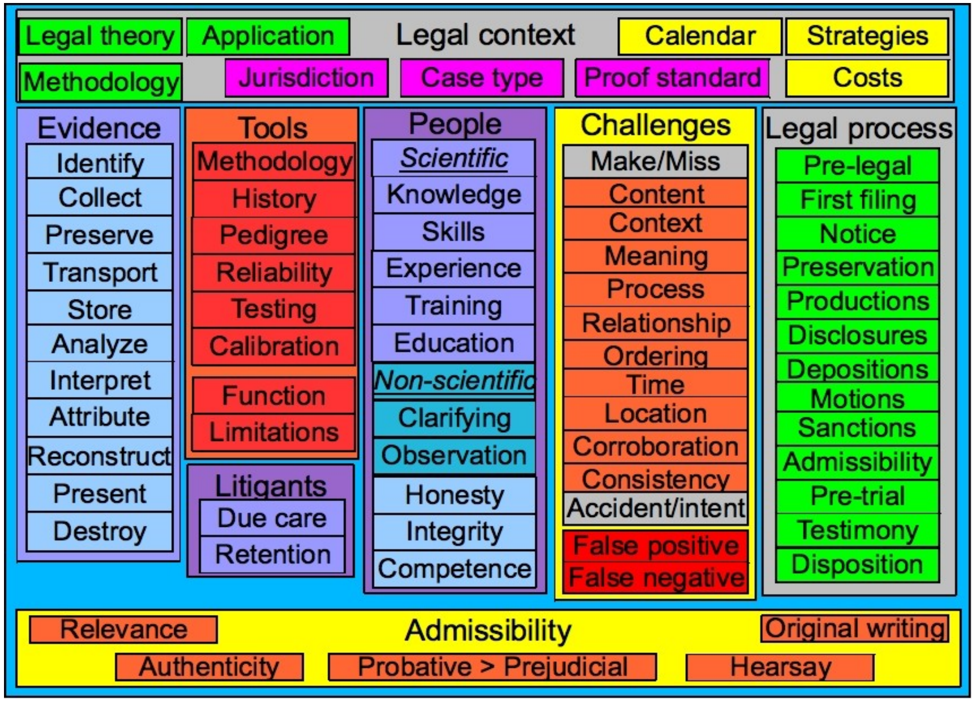
Copyright © Fred Cohen – 1977-2008

<<<------------------

- Enterprise protection:
  - Assure utility of content
    - To management specified tolerance

- Digital forensics:
  - What happened?
  - To an appropriate legal standard!

------------------>>>



Unfortunately... not the same

- Assure utility of content
  - Keep some of it
  - Tell less of it
  - Get rid of some of it
  - Limit costs/complexity
  - Perfect = enemy of good
- Management tolerance
  - What's important?
  - How important?
  - To the business!!!

- What happened
  - All that happened
  - Nothing that didn't
- Legal standard
  - Testimony / expert reports are NOT internal reports
  - Chain of custody and depend on it for business use
  - Reliable methods properly applied

Case example 1

- R&D effort in ~2000
- Very few records of effort were kept
- Executives found guilty of frauds unrelated to this issue in early 2000s
- Migration from one archive to another in 2004 (tossed old)

- Law suit in 2008
- Order to preserve records from 2000
- Records mostly gone by 2008
- R&D largely undocumented
- Select emails recovered by individual workers

The courts and forensics experts have to sort this all out

Case example 2

- Activities took place in early 2000s
- Several large ISPs who don't keep old records
- Anonymizer service with contracts
- Postings to Internet forums and private records as evidence

- Legal case in 2008/9
- Party apparently reading opponent's email with lawyers
- Subpoenas yielded partial information
- “Experts” posted “evidence” and findings to Internet forums before court

A media circus resulted and the case went a different way

Case example 3

- Issue from Dec 1999
- Y2K backups meticulously made
- Corporate backups kept in basement of World Trade Center
- 9/11/2001 happens
- Business continuity adequate to keep going

- Legal case in 2003+
- Records subpoenaed
- Unfortunately...

<<<-----------------

- Fragments of data from around the World used in case
- Couldn't reliably establish events

Guilty verdict overturned and directed not guilty issued

Case example 4

- The “WayBack” machine
  - Used to see what was apparently on the Web in the past
  - Some folks see an apparent violation of a contract, etc.
  - It's “evidence” of wrongdoing!!!
  - They sue thinking they have the smoking gun

- Legal cases have had rulings both ways!!!
  - The WayBack Machine is NOT reliable on its face
  - BUT... some of it is reasonably reliable for some purposes...
  - You NEED and expert to tell
  - And to testify!

The legal standard is very different from the Internet one

Qualifications differences

- Certified [Encase / FTK / whatever] examiners
  - 5-day course and test
- Familiar with corporate information security
  - Operate enterprise defensive systems
  - "Catch" folks to support HR actions
- Any good as digital forensics experts?

- Legal "experts" need knowledge, skills, experience, training, and education
- Ph.D. in relevant field
- Publish peer-reviewed relevant research in journals and books
- Reliable scientific methods properly applied

The legal and corporate standards are very very different

Mediated discovery views

- Electronic discovery
  - A now necessary and undesired expense and risk
  - Mediated discovery could reduce costs
  - We could negotiate with a non-lawyer
  - It could reduce risks
  - If we fool the one person we win
  - Bribes have worked before

- Legal issues (mediated)?
  - Self-incrimination
  - Discovery discretion away from judges
  - Lose right to confidential and independent experts
  - Too few mediators exist
  - Potential for abuse
  - Forces counsel to reveal strategies
  - May actually cost more

The legal and corporate views may be directly at odds

Some other differences

- Often legal to search without substantial limit
- Often actions based on unrelated data (fire them for something else)
- DMCA permits reverse engineering (research)
- Minimal effort to get to a decision is often desired
- Executive management decides what to do and often acts in their own best interest without scrutiny / opposition

- Searches almost always require warrants and are limited in scope
- Process limits actions to relevant issues
- DMCA prohibits reverse engineering in forensics
- High dollar valued cases are often fully litigated
- Opponents fight it out, judge rules in the public interest, deep scrutiny

The two worlds have very different rules and constraints

Some things to think about

- This talk does not provide answers
  - As a keynote - it asks questions
- The talks in this conference will help to get at many of the issues and answers
  - What are the tensions between “security” and “forensics” in the corporate World
  - Intrusion detection and response vs. attribution to a legal standard
  - Electronic discovery – a huge deal – is it one that can be left to “mediators”?
  - Who/what is an “expert” suitable to the corporate vs. legal domain?

Listen carefully...

- The same words mean different things in the legal and corporate context - examples:
  - Forensics (legal) is NOT forensics (corporate)
  - Search (legal) is NOT search (corporate)
- The standards are very different
  - Experts have very different standards
  - Tools have very different standards
  - Evidence had very different standards
- Corporations rarely use science for security
  - Courts rely on scientific studies and bases – corporate “security” rarely uses science at all!

Thank You

http://calsci.org/ - calsci at calsci.org

http://all.net/ - fc at all.net