SARA and Standards of Practice

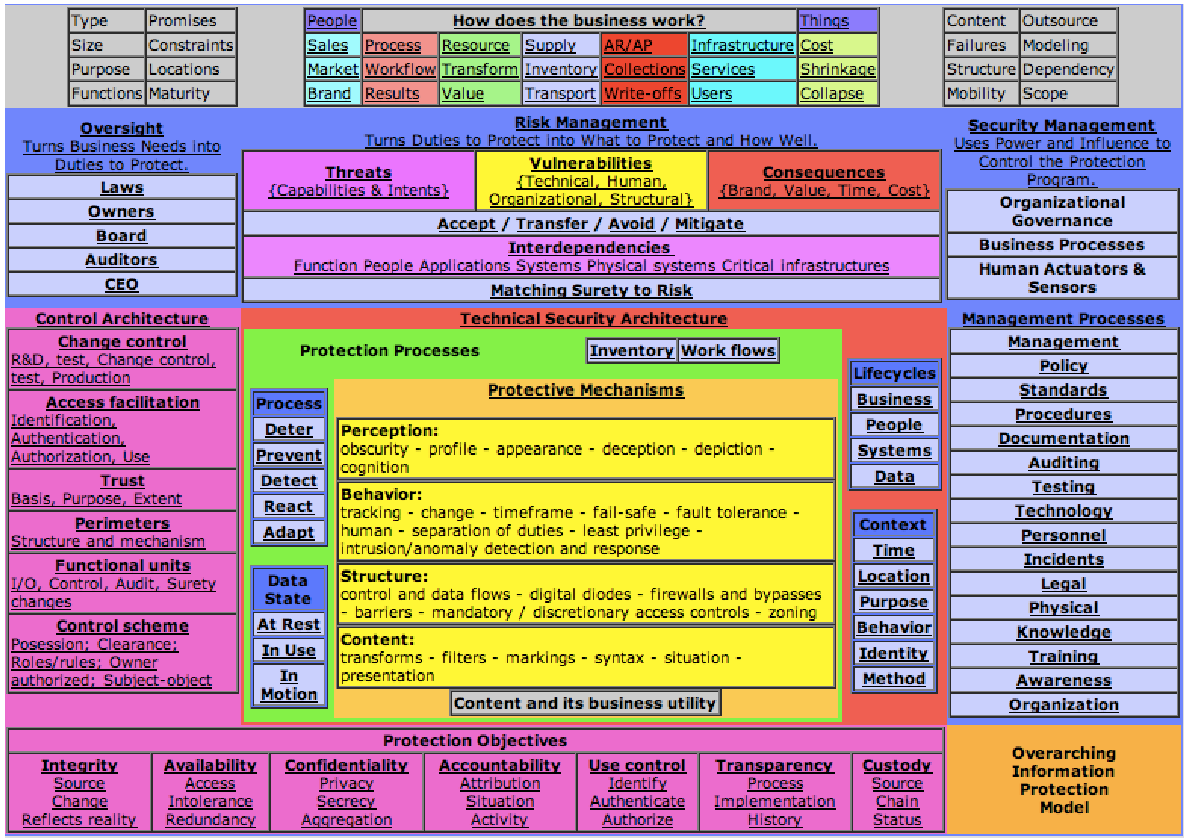
2014-09-17

The ICS-ISAC SARA Conference

Dr. Fred Cohen

Outline

- Situation Awareness Reference Architecture
  - **Identity**, Inventory, Activity, Sharing
    - Standards of Practice (SoP)
  - Specify & review – separation of duties – independence



Type	Promises
Size	Constraints
Purpose	Locations
Functions	Maturity

People	How does the business work?					Things
Sales	Process	Resource	Supply	AR/AP	Infrastructure	Cost
Market	Workflow	Transform	Inventory	Collections	Services	Shrinkage
Brand	Results	Value	Transport	Write-offs	Users	Collapse

Content	Outsource
Failures	Modeling
Structure	Dependency
Mobility	Scope

Oversight
Turns Business Needs into Duties to Protect.
Laws
Owners
Board
Auditors
CEO

Risk Management
Turns Duties to Protect into What to Protect and How Well.
Threats {Capabilities & Intents}
Vulnerabilities {Technical, Human, Organizational, Structural}
Consequences {Brand, Value, Time, Cost}
Accept / Transfer / Avoid / Mitigate
Interdependencies
Function People Applications Systems Physical systems Critical infrastructures
Matching Surety to Risk

Security Management
Uses Power and Influence to Control the Protection Program.
Organizational Governance
Business Processes
Human Actuators & Sensors

Control Architecture
Change control
R&D, test, Change control, test, Production
Access facilitation
Identification, Authentication, Authorization, Use
Trust
Basis, Purpose, Extent
Perimeters
Structure and mechanism
Functional units
I/O, Control, Audit, Surety changes
Control scheme
Posession; Clearance; Roles/rules; Owner authorized; Subject-object

Technical Security Architecture
Protection Processes
Inventory | Work flows
Process: Deter, Prevent, Detect, React, Adapt
Data State: At Rest, In Use, In Motion
Protective Mechanisms
Perception:
obscurity - profile - appearance - deception - depiction - cognition
Behavior:
tracking - change - timeframe - fail-safe - fault tolerance - human - separation of duties - least privilege - intrusion/anomaly detection and response
Structure:
control and data flows - digital diodes - firewalls and bypasses - barriers - mandatory / discretionary access controls - zoning
Content:
transforms - filters - markings - syntax - situation - presentation
Content and its business utility
Lifecycles: Business, People, Systems, Data
Context: Time, Location, Purpose, Behavior, Identity, Method

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

Protection Objectives						
Integrity Source Change Reflects reality	**Availability** Access Intolerance Redundancy	**Confidentiality** Privacy Secrecy Aggregation	**Accountability** Attribution Situation Activity	**Use control** Identify Authenticate Authorize	**Transparency** Process Implementation History	**Custody** Source Chain Status

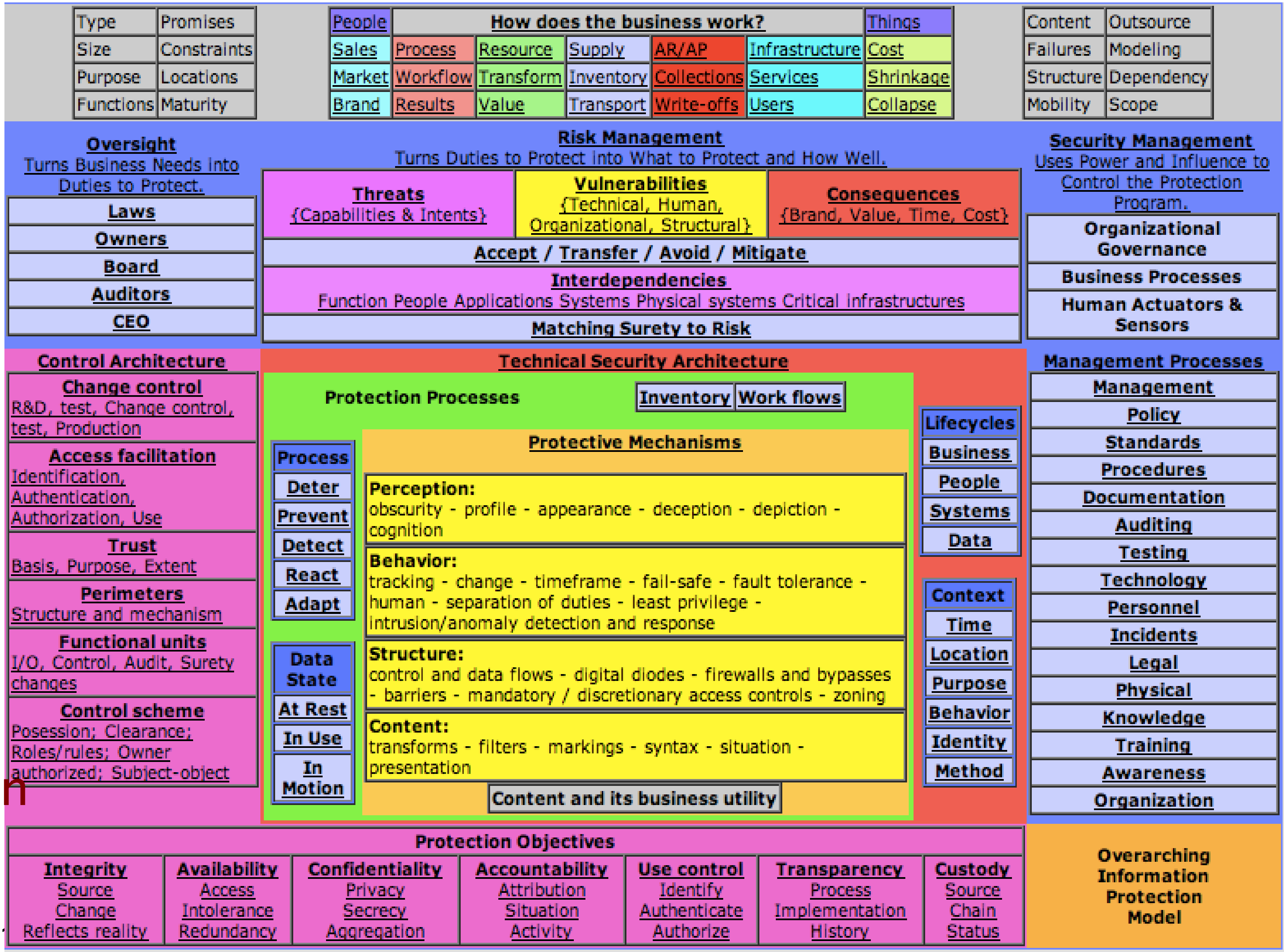
Overarching Information Protection Model

Fearless Security

You have nothing to fear but fear itself

Situation Awareness Reference Architecture

- Identity
  - Context
    - SoP
- Inventory
- Activity
- Sharing
- All.net
  - Protection
    - SoP



Type	Promises
Size	Constraints
Purpose	Locations
Functions	Maturity

People	How does the business work?					Things
Sales	Process	Resource	Supply	AR/AP	Infrastructure	Cost
Market	Workflow	Transform	Inventory	Collections	Services	Shrinkage
Brand	Results	Value	Transport	Write-offs	Users	Collapse

Content	Outsource
Failures	Modeling
Structure	Dependency
Mobility	Scope

Oversight
Turns Business Needs into Duties to Protect.

Laws

Owners

Board

Auditors

CEO

Risk Management
Turns Duties to Protect into What to Protect and How Well.

Threats
{Capabilities & Intents}

Vulnerabilities
{Technical, Human, Organizational, Structural}

Consequences
{Brand, Value, Time, Cost}

Accept / Transfer / Avoid / Mitigate

Interdependencies
Function People Applications Systems Physical systems Critical infrastructures

Matching Surety to Risk

Security Management
Uses Power and Influence to Control the Protection Program.

Organizational Governance

Business Processes

Human Actuators & Sensors

Control Architecture

Change control
R&D, test, Change control, test, Production

Access facilitation
Identification, Authentication, Authorization, Use

Trust
Basis, Purpose, Extent

Perimeters
Structure and mechanism

Functional units
I/O, Control, Audit, Surety changes

Control scheme
Posession; Clearance; Roles/rules; Owner authorized; Subject-object

Technical Security Architecture

Protection Processes

Inventory | Work flows

Process: Deter, Prevent, Detect, React, Adapt

Data State: At Rest, In Use, In Motion

Protective Mechanisms

Perception:
obscurity - profile - appearance - deception - depiction - cognition

Behavior:
tracking - change - timeframe - fail-safe - fault tolerance - human - separation of duties - least privilege - intrusion/anomaly detection and response

Structure:
control and data flows - digital diodes - firewalls and bypasses - barriers - mandatory / discretionary access controls - zoning

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

Content and its business utility

Lifecycles: Business, People, Systems, Data

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

Management Processes

Management

Policy

Standards

Procedures

Documentation

Auditing

Testing

Technology

Personnel

Incidents

Legal

Physical

Knowledge

Training

Awareness

Organization

Protection Objectives

Integrity	Availability	Confidentiality	Accountability	Use control	Transparency	Custody
Source	Access	Privacy	Attribution	Identify	Process	Source
Change	Intolerance	Secrecy	Situation	Authenticate	Implementation	Chain
Reflects reality	Redundancy	Aggregation	Activity	Authorize	History	Status

Overarching Information Protection Model

Why is identity so important?

- Without the context, decisions are meaningless
  - How do you know what to share if you don't know why?
  - How do you know what to look at/for without context?
  - What will you do with the information when/if you get it?
- It's all about the business
  - The utility of content drives the identity process
    - What is the utility?
    - How do we assure the utility?
    - What do we do when the utility breaks down?
    - How far are we willing to let it break down?
    - In the face of what threats?
    - To what business advantage?

We apply Standards of Practice

- What is a (our) Standard of Practice (SoP)
  - An SoP is **not** a “Standard” (something you follow)
  - “Reasonable and Prudent” practices (diligent vs. negligent)
    - **Not the ONLY such practices** – not always applicable
  - Open source/reviewed: http://all.net/ → Protection → SoP ...
- We use the standard of practice to help our experts
  - Ask a reasonably comprehensive set of questions
  - Codify responses consistently in a defined language
  - Guide decisions using pre-defined bases (rote vs. real)
  - Identify variances from baselines for consideration
- When the standard practice works, we use it
  - When it doesn't, we adapt, and update if/as appropriate

SoP on the Web

- Live demonstration of the ICS SoP
  - Other SoPs
    - Enterprise – started in the 1990s
      - Applied to hundreds of enterprises over many years
      - Metrics gained from efforts are useful for various purposes
    - Archives and Records Management (ARM)
      - Being developed in cooperation with ITrust out of UBC
      - Currently pending the 1st two archives → more to come
      - Building a simple sample (rote) compliant archive
    - Cyber Insurance – the context required to determine rates
      - Working with RISCO, Lloyds, others
      - Using SoP as baseline and fusing with actuarial data
  - Scientific research as a basis
    - A long way to go – and the Webster CyberLab …

Thank You

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