Fred Cohen & Associates

Specializing in Information Protection Since 1977

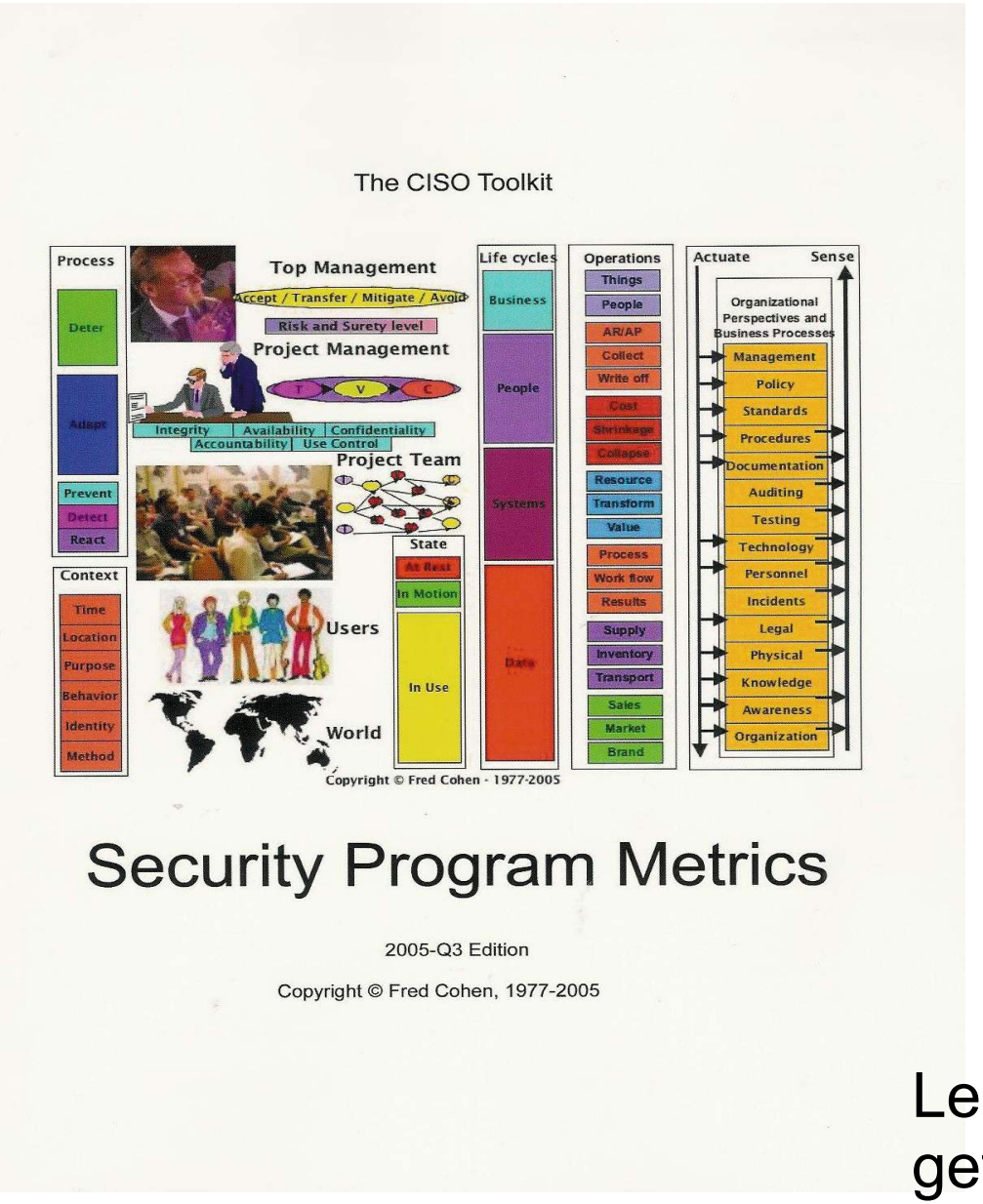
Fred Cohen

Fred Cohen & Associates

2005-11-14

CSI Conference

# Security Metrics




Leave me your business card and
get a chance at a free security mentoring

# What does Fred know about security metrics anyway?

- Some metrics work in the early 1990s
  - Relativistic risk assessment
  - Protection posture assessment metrics
- Looking seriously at security metrics in the late 1990s
  - Research in deception for protection
  - Led to the need to measure quality of defenses
  - Resulted in a new metric
    - Progress in an attack graph as f(time)
  - Good for the particular measurement but...
- A desire for more serious consideration
- Some general disgust at scanning metrics and so forth

# And then what?

- Development of IPPA comparisons
  - Many protection posture assessments done
  - Comparisons across about 150 areas
  - Comparisons done for enterprises as add-on
- The CISO ToolKit
  - Developed “Governance Guidebook” with common basis for enterprise security architecture
  - Added top-down metrics for enterprises
  - Developed “Security Metrics” to support it
  - Developed more specific metrics and guidance
    - Startup, Diligence, Typical, Excellent, Best ratings
    - Things you can count

# Outline

- What makes a good metric
- Examples of not so good metrics and why
- Examples of better metrics
- Program-wide metrics with roll-up
- Measuring your program
- Summary / Questions / Comments?

# What makes a good metric?

- To understand this we must understand why people want metrics
  - You wouldn't want security if you didn't need it
  - If you have to have it you have to manage it
  - You can't manage what you can't measure
  - Measurement works best with metrics
  - But you can use other measures if you have to
- So the idea is to measure things so you can manage them
- So what do I manage?
  - Time for a model

# Enterprise Information Security Architecture

## How does the business work?

| People | | | | | | 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 |

## 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

What to protect

Risk and Surety Level and Matching

## 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

- Identification
- Authentication
- Authorization
- Use

- Perimeters

**Functional Units**

Less sure — Control → I/O → Audit — More sure

**Access Controls**

Clearance — Classification — Less — More — Consequences

## Technical Security Architecture

**Process**
- Deter
- Prevent
- Detect
- React
- Adapt

**Protection Processes**

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

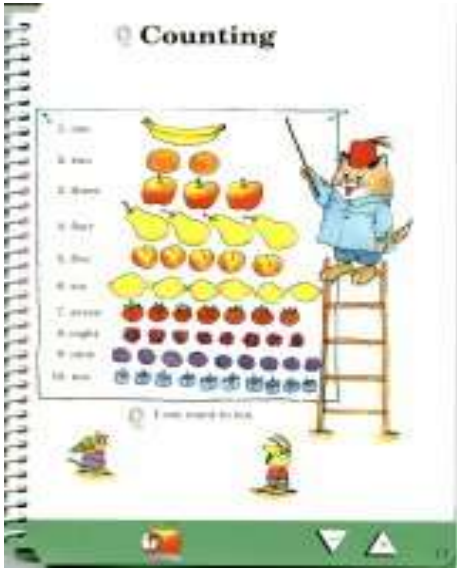
**Data State**
- At Rest
- In Use
- In Motion

## Objectives

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

# What should you measure?

- Assume:
  - You can only measure things you can count
- Count the things in your model
  - What can we count from it?
  - Start at the top and work down
  - Drill down for more details and accuracy
- You want repeatable measurements
  - Independently repeatable with the same results
  - That can be compared over time
  - That can be compared across enterprises
- Goal depends on the model
  - In this one, meeting the duty to protect is good
  - You might want to measure costs... not so easy



# Outline

- What makes a good metric
- Examples of not so good metrics and why
- Examples of better metrics
- Program-wide metrics with roll-up
- Measuring your program
- Summary / Questions / Comments?

# Not so good metrics

- Building hills to the moon
  - a.k.a. Constant improvement of something
- I will manage what I can easily measure!
  - a.k.a. Shooting at the wrong target
- I will measure what I can and manage something else
  - a.k.a. A disconnect
- Return on Investment (ROI) strategies
  - If nothing went wrong what does it mean?
  - If lots of things went wrong, what does it mean?
  - If the worst case loss is out-of-business, do I get that as the ROI every year, month, week, day?

Text face / Browser / EDI
Disk / File encrypt
Java / Application
VPN / FW / Access control
Authentication
TCG / TCSEC
Audit / Check
AV / AS / A-Trojan / A-spy
I / A / C / Use / Acct

# Outside

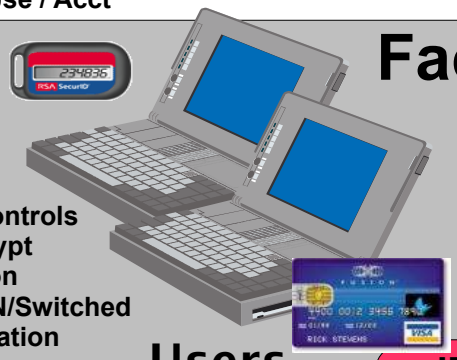
Control

Audit

## ISP
AS / AV / A-Trojan / A-spy
SMTP Gateway / IdM
QoS / Hosting / Crypto
Authentication / 3rd party
File sharing / Certificates

## Vendor
Update / Test / Patch
Help desk / Document
Search / Fuse / Test
Track / Trace / Up-Down
Performance measure

# Facilities



## FW
Router / Switch / Gateway
DMZ / Proxy / VPN
Authenticate / IdM interface
HW accelerated / Appliance
{Good/Bad} x { Ingress/Egress}

## NOC
Collect / Normalize
Fuse / Aggregate / Store
Present / Predict / Alert / React
Administrator console
Surveillance system
Control system

## Other Sites
Query limits
Redundancy
Roles and rules
IdM interface
Federation
Aggregation control
Change management
Code validation
Access controls
VPN
Authentication
Audit
Separation of duties
IDRS
Firewalls
Wireless

## Users
Access controls
Disk encrypt
Application
VPN/VLAN/Switched
Authentication
Audit
Separation of duties

Control

IDRS

Firewall

Audit

## Data Center
Query limits
Access controls
Audit
Redundancy
Separation of duties
Roles and rules
IdM interface
Aggregation control

IDRS

Apps

Change

Access controls
Audit / Testing
Separation of duties
Code validation
Change management

Authentication
Separation of duties
Code validation
Change management
Access controls
Application
Audit
VPN
VLAN
Switched

R&D

## Application/DB Programmers

Query limits
Access controls
Audit
Redundancy
Separation of duties
Roles and rules
IdM interface
Aggregation control
Change management
Code validation

Firewall

IDRS

Apps

Control

IDRS

Firewall

Audit

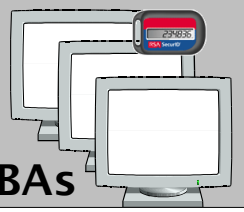
Query limits
Access controls
Audit
Redundancy
Separation of duties
Replay and rollback

Data-bases

Change

R&D

Access controls
Audit
Separation of duties
Code validation
Change management



## DBAs

Control

IDRS

Firewall

Audit

Control

## Users
Access controls
Authentication
Audit
Separation of duties

Redundancy
Separation of duties
Backups

SAN

## Administration

Encryption
Backups
Failover

## Data Center

Audit

## Trading Partners
Query limits
Redundancy
Roles and rules
IdM interface
Federation
Aggregation control
Change management
Code validation
Access controls
VPN
Authentication
Audit
Separation of duties
IDRS
Firewalls
Wireless

# Outline

- What makes a good metric
- Examples of not so good metrics and why
- Examples of better metrics
- Program-wide metrics with roll-up
- Measuring your program
- Summary / Questions / Comments?

# Things we can count

- As an example: things about people
  - How many people do we have?
  - How many have had background checks?
  - How many should have had them?
- What are good properties of a metric?
  - Anyone can count everything easily
    - Evidence is in physical HR files
  - A reasonable goal
  - Based on the "gap" you have reasonable options
    - Fire the ones without the checks
    - Stop them working on sensitive stuff till completed
    - Punish the HR person who failed to do their job ... etc.
- Are there any problems with it?

# Counting problems

- Size of the problem
  - There might be a lot of them
  - It might be expensive to count them
  - Counting might not be really accurate
  - But statistics can do a lot to solve size problems
- What does it tell us about the effectiveness?
  - It tells us that we are doing the things we think should be done
  - It does not tell us whether it worked or is working
- Big assumption:
  - If you do the job properly, you will have an effective protection program

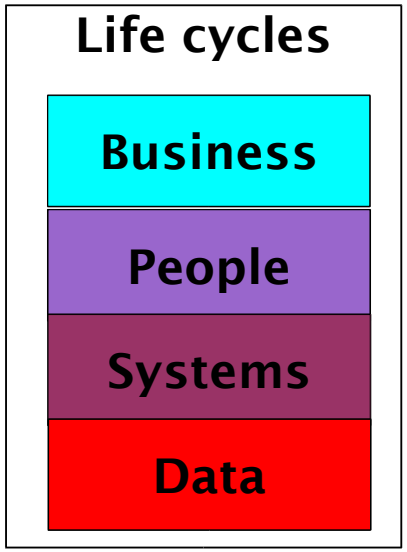
# Hidden costs?

- Time to authenticate
- Performance degradation from encryption
- Time spent helping others with security issues
- Time spent reporting or responding to incidents
- Time spent in security awareness training not charged back
- Cost of extra software for security requirements
- Installation, maintenance, and update time for security software
- Time delays in booting up or logging in from security scans, etc.
- Delays while running programs for security-related issues
- Costs of multiple authentications after initial sign-on
- Help desk calls related to lost passwords
- Costs of having to shut down and restart for security reasons
- Time wasted during security-related outages of systems or networks
- Time spent in backups not centrally managed and accounted for
- Time spent in security-related documentation
- Time spent reviewing security-related policies and reading contracts
- Time spent in gaining additional approvals for exceptions
- Cost of delays associated with authentications for external access
- Relationship costs because of security requirements met and unmet

# Counting life cycles

- How do we assure that security meets all requirements at all phases of all life cycles?
- What are the issues? Start counting things!

**Enterprise security model**
**-> Executive security management**
**-> Lifecycles**




**Business**

Formation
Funding
Operation
IPO
Joint Venture
Merger
Acquisition
Divestiture
Bankruptcy
Dissolution

**People**

Conception
Pregnancy
Birth
Education
Marriage
Divorce
Training
Hiring
Promotion
Demotion
Suspension
Vacation
Illness
Leave
Job change
Move
Resignation
Termination
Retirement
Death
Legacy

**Systems**

Conception
Design
Engineering
Implementation
Operation
Maintenance
Disaster
Recovery
Upgrades
Transformation
Consolidation
Obsolescence
End-of-life
Reconstitution
Resale
Destruction
Recycling

**Data**

Inception
Observation
Entry
Validation
Verification
Attribution
Fusion
Separation
Analysis
Transformation
Transmission
Storage
Use
Presentation
Modification
Loss
Recovery
Reconstruction
Backup
Restoration
Destruction

# Drill down further

**Enterprise security model**
**-> Executive security management**
**-> Lifecycles**
**-> Business lifecycles**

- Business lifecycles
  - Mergers and acquisitions
    - Due diligence takes security issues into account (list of specific issues)
    - Firewalls are put between entities to allow cooperation while the protection infrastructures are reconciled
    - Classification systems, clearances, and need-to-know are reconciled to gain proper controls
    - Interdependency analysis, risk aggregation, and business continuity and disaster recovery plans are reconciled
    - Disgruntled and laid off employees are properly taken care of within this process (see people->disgruntled)
- You can count them all
- They are all meaningful in the model

# But so what?

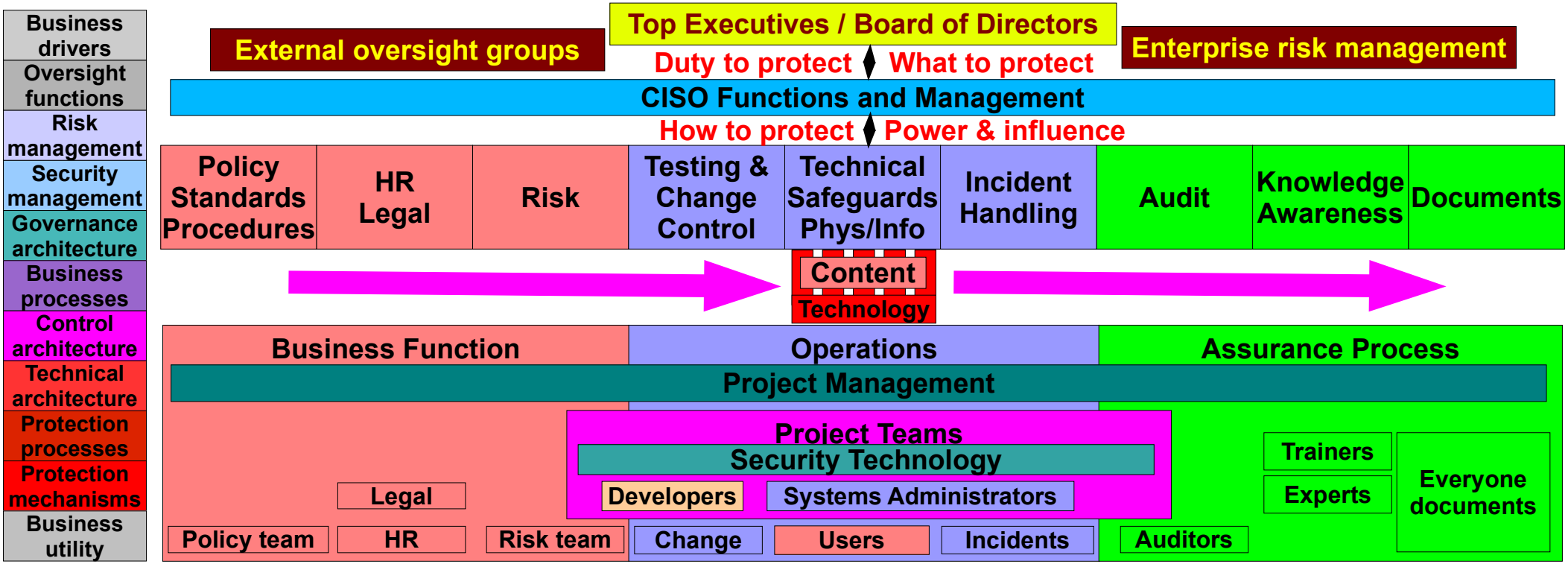
- How do they provide utility?
  - They tell you how well the program is doing
  - They allow you to measure against goals
  - They have finite accomplishable objectives
  - Executive management can set desired levels
- Is there a basis for comparison?
  - Relative scores with internal or external basis
    - Startup
    - Diligence
    - Typical
    - Excellent
    - Best
- But there sure are a lot of them!

# Outline

- What makes a good metric
- Examples of not so good metrics and why
- Examples of better metrics
- Program-wide metrics with roll-up
- Measuring your program
- Summary / Questions / Comments?

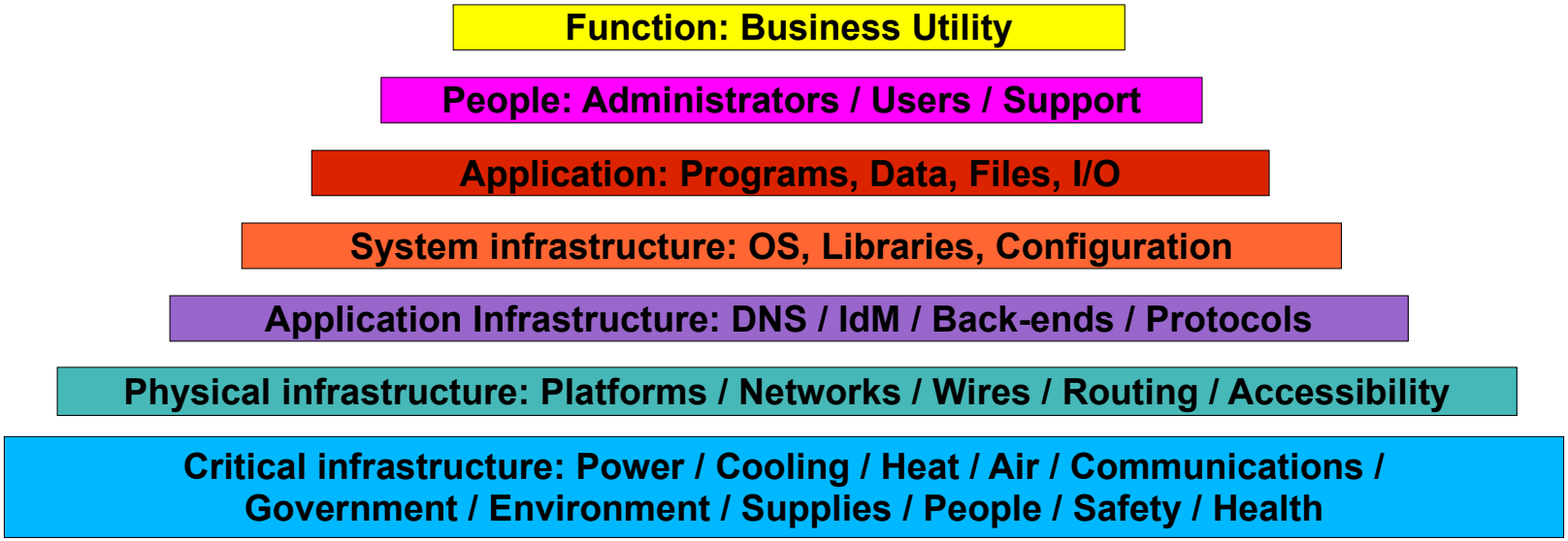
# Program-wide metrics

- Start at the top with a business model
- Use duty to protect as the top-level feedback
  - Measure fulfillment of duties to protect
  - Drill-down into duties as far as you need to
  - Human and automated sources and measurements



# Risk aggregation example

- What are we counting?
  - Total risk placed on individual components
  - Worst case consequence of protection objective loss
- Interdependencies and risk aggregation
- Does it meet management thresholds?



# Risk aggregation metrics

**Enterprise security model**
**-> Business risk management**
**-> Interdependencies**
**-> Risk aggregation**

- Top level measurements
  - Management defined consequence thresholds are used for risk levels.
  - Risk aggregation is analyzed in low risk environments.
  - Risk aggregation is analyzed in medium risk environments.
  - Risk aggregation is analyzed in high risk environments.
  - Aggregated risk is mitigated by increasing surety levels.
  - Aggregated risk is mitigated by partitioning the risk area.

# Drill-down for risk aggregation

**Enterprise security model**
**-> Business risk management**
**-> Interdependencies**
**-> Risk aggregation**
**-> Drill-down**

- Risk aggregation analysis
- Single points of failure
- Radius-driven common-mode failures
- Other common-mode failures
- Key individuals

# Further down

**Enterprise security model**
**-> Business risk management**
**-> Interdependencies**
**-> Risk aggregation**
**-> Radius-driven common-mode failures**

- Except as approved on a case by case basis by the CEO, within a radius of effect associated with the attack mechanisms within the capabilities of the threats identified in threat assessment, no single event is able to cause medium or high consequences.
- Natural effects within reasonably expected and historically supported radii are taken into account in risk management.
- Redundant data centers in the same Earthquake zone or flood zone are not used to support the claim to have no single point of failure.
- Redundancy within a single building or location is not used to claim no single point of failure for a medium or high consequence situation.
- High consequence radius-based risk acceptance is reviewed by the CEO at least once every 6 months.
- Medium consequence radius-based risk acceptance is reviewed by the CEO at least once every year.

# How do I count it?

- Natural effects within reasonably expected and historically supported radii are taken into account in risk management.
  - It measures the risk management process
  - Review the process for ALL analyses (A)
    - Count number that include radius vs. not
      - For those that do: (X)
        - Count the number that use histories / total that do it (H)
        - Count natural effects considered / total list of natural effects (E)
- Result (out of 10) = 10*Sum(Hx*Ex)/A

# Outline

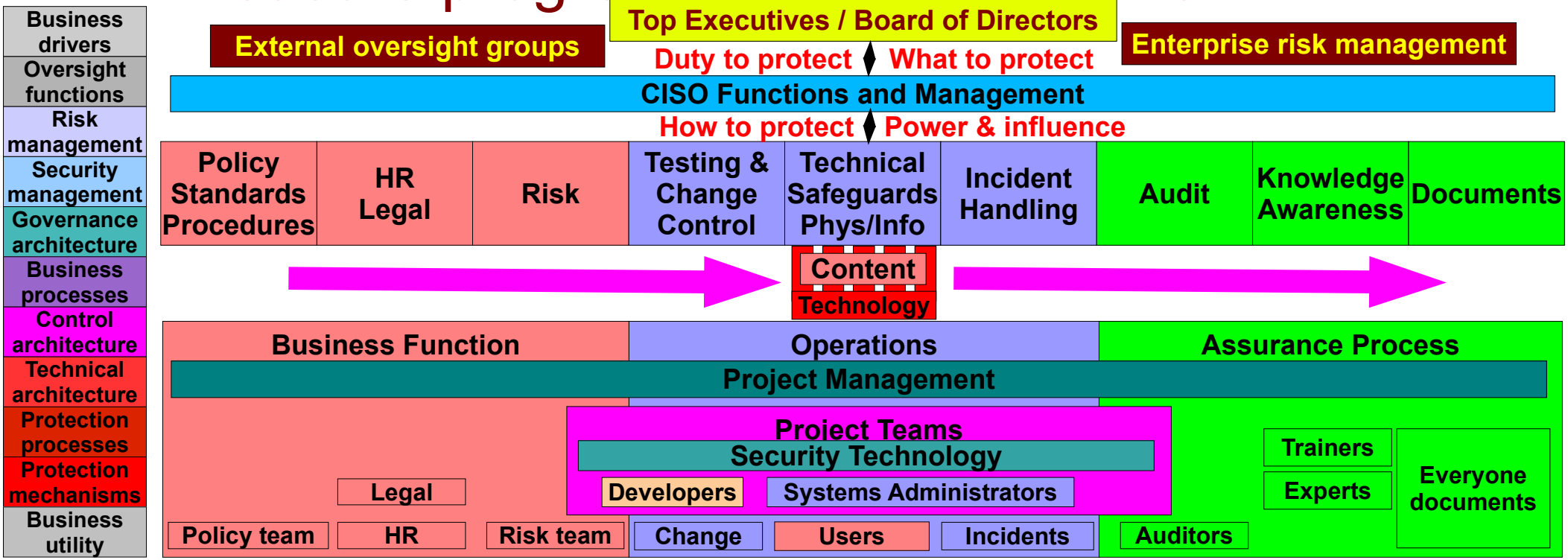
- What makes a good metric
- Examples of not so good metrics and why
- Examples of better metrics
- Program-wide metrics with roll-up
- Measuring your program
- Summary / Questions / Comments?

# Start working

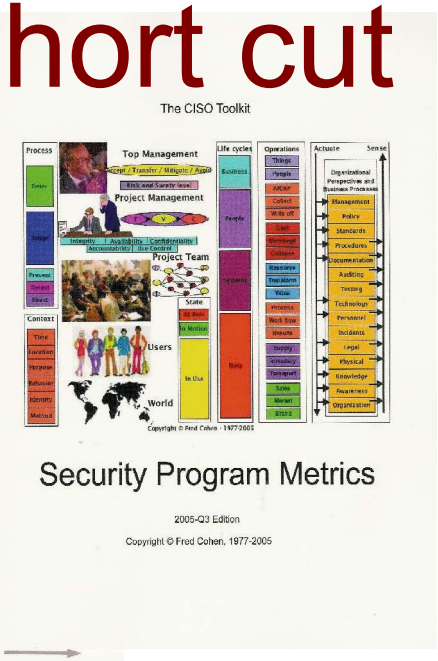
- Your task list:
  - Make a good enterprise security management model and detail it out to a desired level
  - For each element of it, top down, build a set of countable things to measure
  - Measure these in many places and against many standards to generate desired measured values
  - Measure your program to the depth desired
    - More depth = more resources
    - It grows quickly
  - Find the gaps and fill them
    - It's easy – just figure how much to add to get to the desired counts and get the system to do it

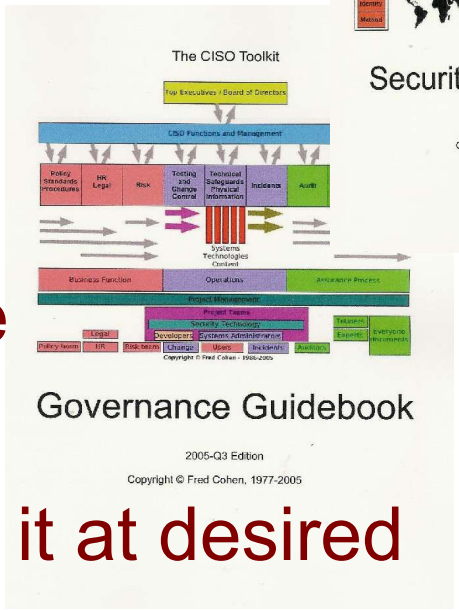
# An enterprise-wide governance issue

- Engage the various CISO-related groups to do their part of the work as your feedback
- Roll-up results into overall performance criteria that are reportable to the CEO
- Measure progress vs. cost over time



# Or take a short cut




- Pick an existing model
  - That suits your enterprise
  - With existing countable metrics
  - In a way that is politically palatable
- Start implementing it
  - Use power and influence to create it at desired depth levels across the enterprise
  - Create roll-up reports periodically as feedback to and on you for the program
  - Update depth and implementation over time as desired to optimize performance

# Outline

- What makes a good metric
- Examples of not so good metrics and why
- Examples of better metrics
- Program-wide metrics with roll-up
- Measuring your program
- Summary / Questions / Comments?

# Summary

- To manage you need to measure
  - Repeatable, independently verifiable, meaningful
  - Measurements of the protection program
  - Measure against meeting duty to protect
  - Don't measure technology, measure process
  - Don't build hills to the moon
  - And of course costs – are not so easy
  - ROI is not sensible – educate top management
- Top down approach advocated here
  - More complexity as you drill further down
  - Use CISO management structure to do it
  - Roll up into reportable CEO-level criteria
  - Demonstrate that duties to protect are met

# Questions? Comments?

Leave me your business card – get a chance at a free security mentoring