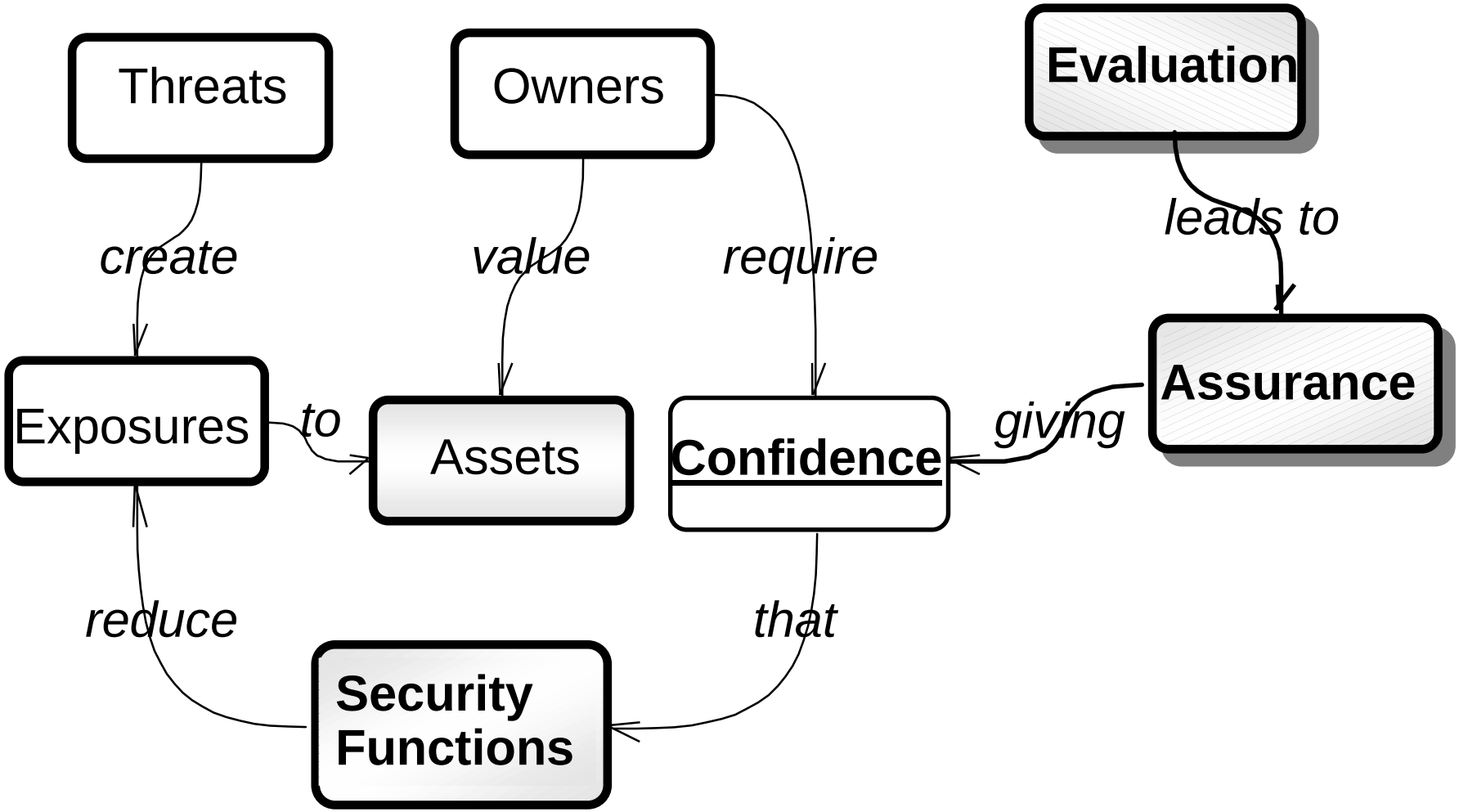
A Security Business Case for the Common Criteria

Marty Ferris
Ferris & Associates, Inc.
202-234-9683
jmferris@erols.com

Outline

- Security Problem Overview
  - Bounding a Moving Target
- Role of Standards
- Common Criteria

Security Concepts and Relationships



Bound the Exposure Problem – Organizational Security Management

- Develop Policies and Standards
- Develop Operational Security Practices
- On-Going Assessment of Security Program

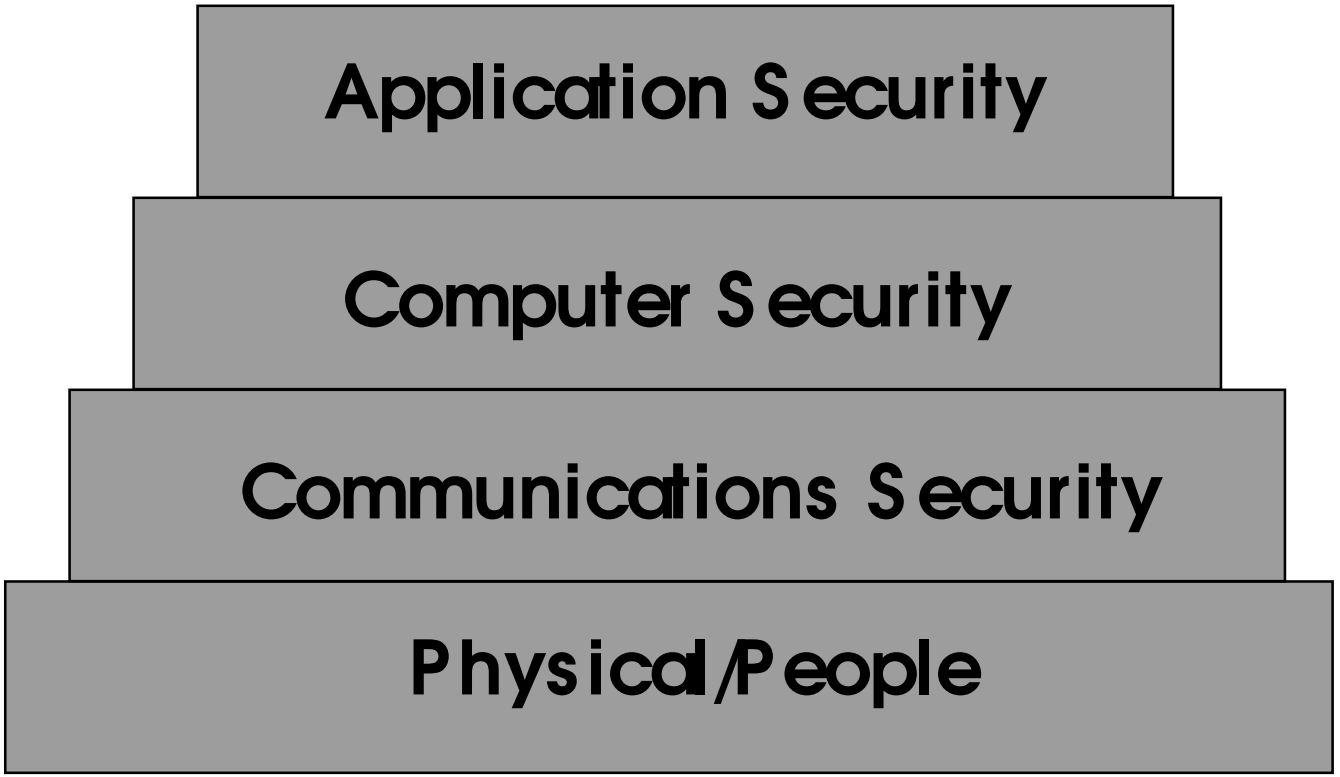
Operational Security Practices
Defining "Good Enough"

- Risk/Acceptability Model
  - Security Program as Starting Place
  - Ongoing assessment and refinement
- Marketplace dependence for IT Security Solutions
- Security Infrastructures Evolve

Security Infrastructures

- Physical Security
- "People" Security
  - Internal Personnel Security
  - Customer's Security Role
- IT Product, Systems and Services Security
- Anomaly Processing
  - Identification of Security Events

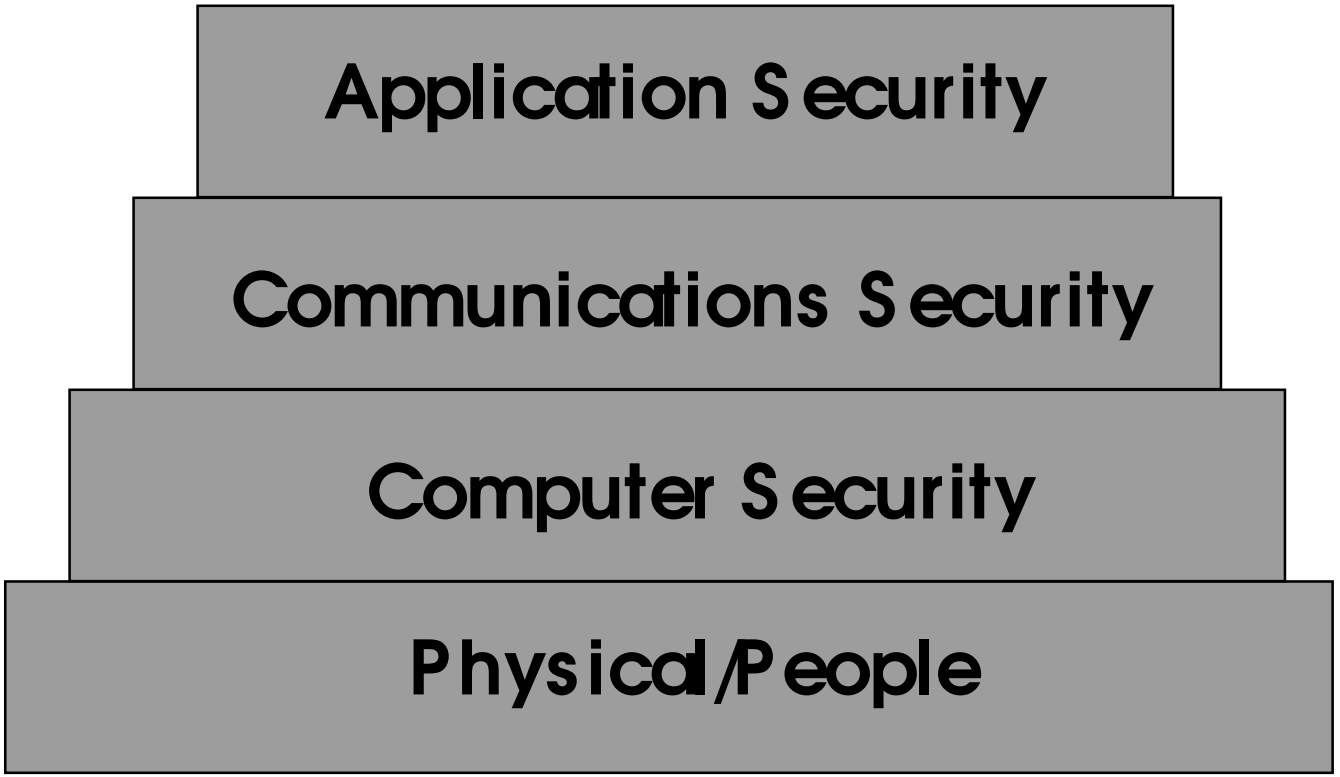
Old Security Infrastructures



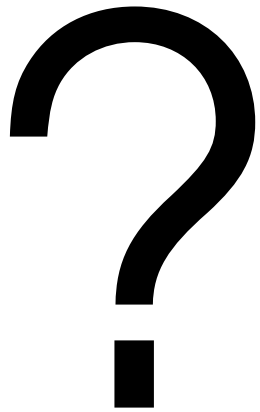
Computer Security-
Central Technical Security Infrastructure

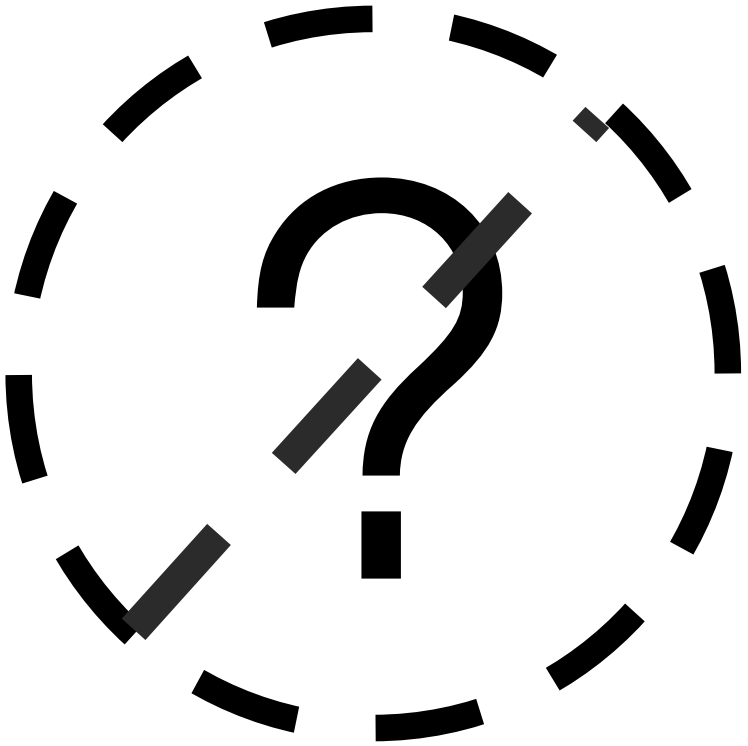
- Application Security
  - Smart Cards
  - Browsers
- Virtual Private Networks
  - Firewalls
  - IPSec
  - TLS/SSL
- Public Key Infrastructure

New Security Infrastructures



Bad Security



Good Security

Security
"Reality"