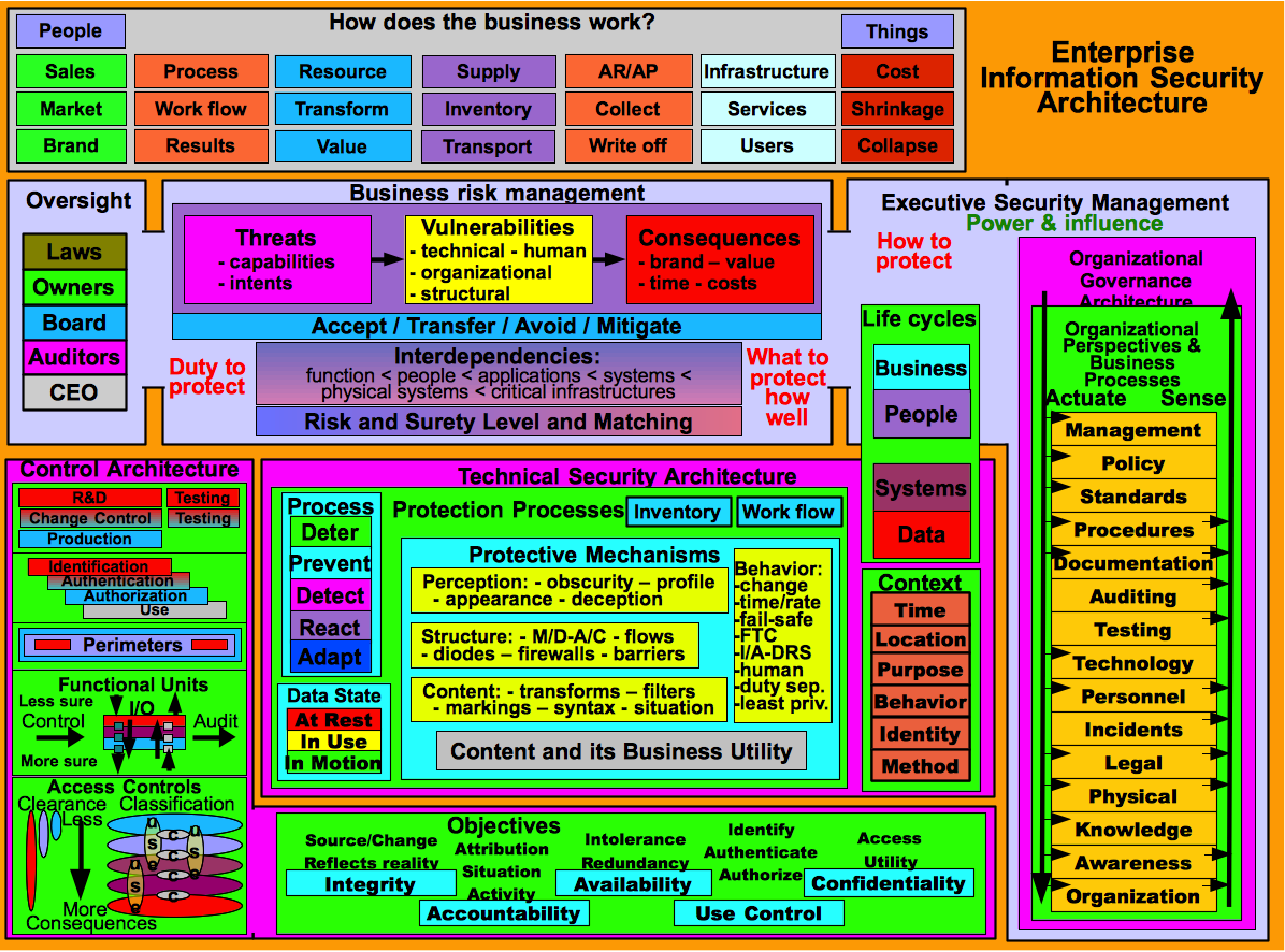
MOBILE COMPUTING SUMMIT

Mobile Computing Summit 2011
Security Workshop

Securing the Mobile Enterprise
Fred Cohen – CEO
Fred Cohen & Associates

Hyatt Regency San Francisco Airport
Burlingame, CA

28 June 28, 2011



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

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

Identification

Authentication

Authorization

Use

Perimeters

Functional Units

Less sure

I/O

Control

Audit

More sure

Access Controls

Clearance

Classification

Less

More

Consequences

S

C

Technical Security Architecture

Process

Deter

Prevent

Detect

React

Adapt

Protection Processes

Inventory

Work flow

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

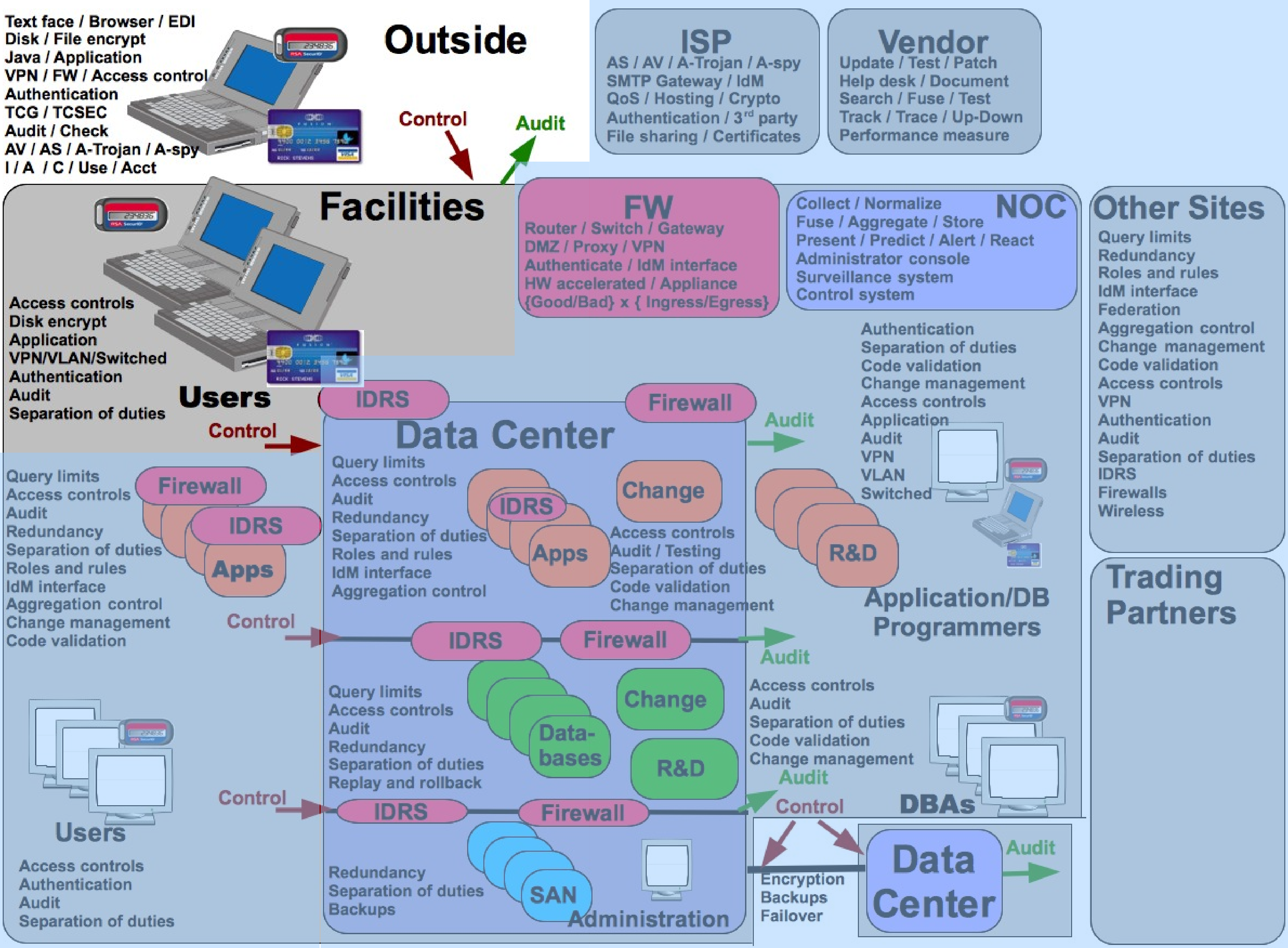
Authorize

Use Control

Access

Utility

Confidentiality



Outside

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

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

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

Users

Control

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

Trading Partners

IDRS

Firewall

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

Audit

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

Audit

Control

DBAs

Users

Access controls
Authentication
Audit
Separation of duties

Control

IDRS

Firewall

Redundancy
Separation of duties
Backups

SAN

Administration

Encryption
Backups
Failover

Data Center

Audit

The overall information security situation today

- The security requirements have not changed
- The “risk” landscape has changed
    - Threats increase with time
    - Vulnerabilities remain / are more exploitable
    - Consequences are essentially unchanged
- Resources for security are relatively decreasing
- Asking the simple questions
    - What can we control?
    - How can we control it?

What can we control?

- We can control lots of things
  - Insider threats, vulnerabilities, risk aggregation, information flows, quality of mechanisms, costs, accepted risks, perceptions of the enterprise, optional promises we make, etc.
- We cannot seem to control our people
  - They are going mobile
  - We can't seem to / we don't want to stop it
- How does “security” say “YES” to mobility?
  - Prioritize!

How can we control it?

- Say yes to mobility
  - When the risk is low
  - When the risk is medium and controllable
  - When it is the best alternative
- Knowing WHEN to say “No”
  - Identify and understand the business and its risks
  - Recognize the rewards from mobility
  - Set reasonable limits that everyone understands
- Knowing HOW to say “Yes”
  - Creative security enablement
  - Removing the barriers to productivity

Case study – Saying YES

- Classified process control facility
  - Scientists need to walk around the facility keeping track of things and making adjustments in near real-time
- Alternatives:
  - Place a classified computer and network every 15 feet and have the scientists log in to each as they walk around, enter the little bit of data, do a calculation, adapt the system, and log back out
  - Have them use mobile classified devices to do the same work at lower cost, more ease of use, more efficiency, and less human resistance

Cast study – Saying YES

- Military field operations
  - Operational military personnel are in the field and need to be able to operate effectively. That includes gaining access to real-time intelligence, targeting, mission planning, ordering explosions at locations at times, etc. - and all that goes with it
- Alternatives:
  - Don't have the advantage of faster tempo, precise targeting, more agility, and lose the war
  - Use mobile computing with secure communications and users who are properly trained and knowledgeable and win the war

Case study – Saying YES

- Major pharmaceutical company high-valued and regulated drug manufacturing lines
  - Need access to process control data and limited ability to "adjust" process w/in pre-defined control parameters. But no "changes" to the line and "incidents" costs $100M+
- Alternatives
  - Permanently colocate 5 shifts of the full range of scientists and engineers with each line
  - Use mobile remote control capability to shift control and data from place to place over time with digital diodes and FSM controls to limit effects

Case study – Saying YES

- Global financial institution with high-valued real-time transaction systems
  - Need to allow trades from authorized individuals from anywhere at any time using whatever device the user wants to use
- Alternatives
  - Lose the globe-trotting wealthy customer to the competition
  - Write applications allowing trades from insecure mobile devices anywhere at any time and provide a more secure submit/commit device for high valued transactions

Case study – Saying YES

- Startup secure cloud computing service (TAP)
  - Need to support secure mobile access to enterprise resources through cloud infrastructure (integrity, availability, confidentiality, use control, and accountability all required)
- Alternatives
  - Each enterprise invests millions of dollars and more each year to create, operate, and manage an end-to-end security architecture for mobile access to enterprise systems
  - A provider creates different surety level endpoint protection environments integrated with cloud-based verification updates and interconnects to enterprise POPs with economy of scale

Case study – Saying NO?

- Nuclear power plant control room operations
  - Need to keep the power plant under control at all times using specialized experts who can use specialized control systems in well trained operational modes and real-time simulation systems for higher risk situations
- Alternatives
  - Permanently colocate 5 shifts of the full range of scientists and engineers at each plant
  - No mobile alternative is currently and reasonably available – BUT when radiation levels are high, why not allow mobility of the control function?

Come the reference architecture

- Each of the examples discussed has
  - Architectural elements
  - Design elements
  - Implementation and operational requirements
- Protection is something you do

  Not something you buy
- Economy of scale comes when you architect one after another and come to understand design patterns across a wide spectrum

If they can do it, why can't you?

- There are always ways to say “YES” to mobility with adequate security
  - If I can do it for classified environments, military systems, real-time industrial control systems, high-valued manufacturing systems, enterprise cloud computing companies, and high-dollar financial transactions, you can do it for almost anything else you want to identify
- But there is a cost to doing the job right
  - Each situation demands a unique look
  - Most cases require a comprehensive understanding and architectural perspective

MOBILE COMPUTING SUMMIT

Thank You

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

ICS: http://fredcohen.net/