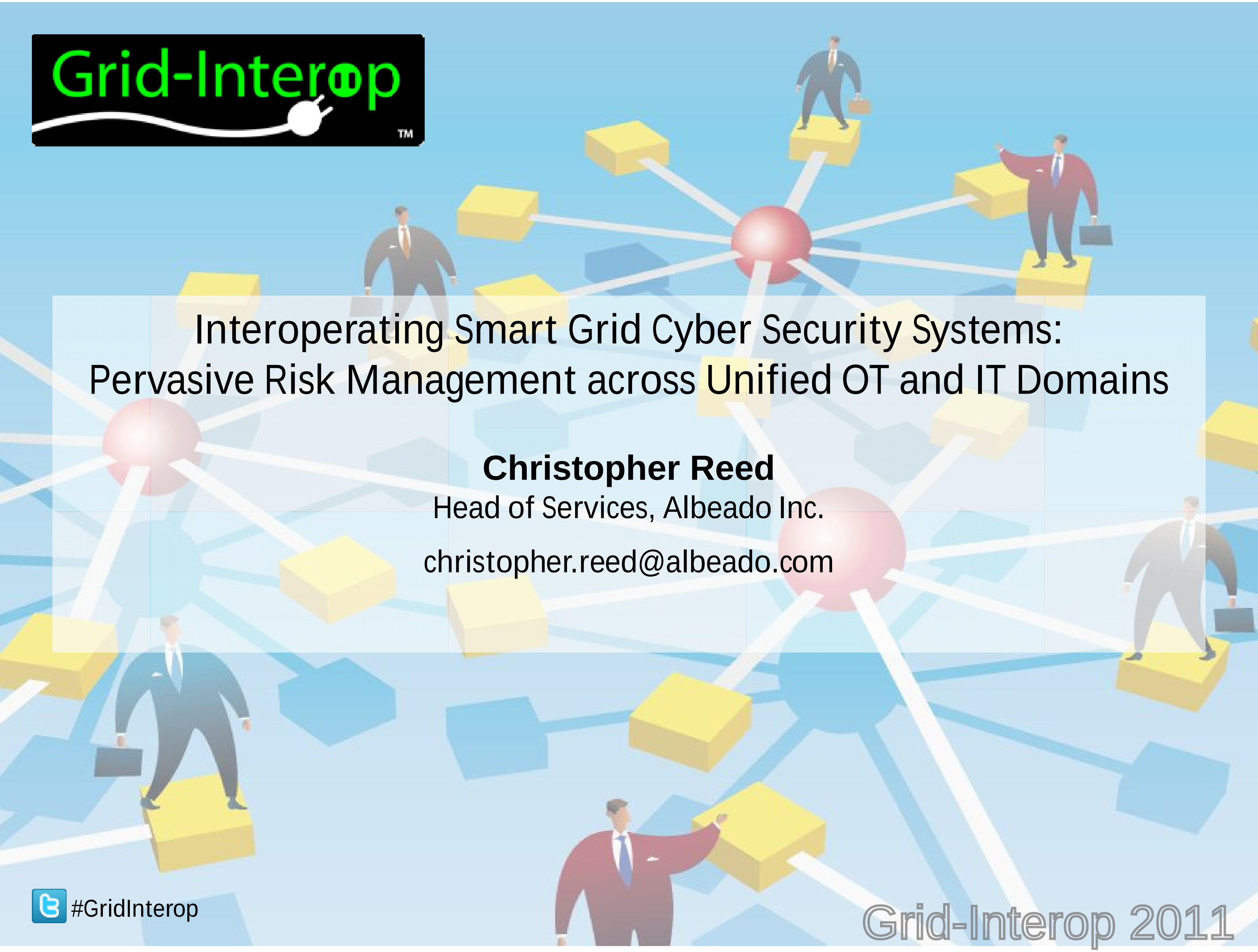
Grid-Interop™



Interoperating Smart Grid Cyber Security Systems: Pervasive Risk Management across Unified OT and IT Domains

Christopher Reed
Head of Services, Albeado Inc.

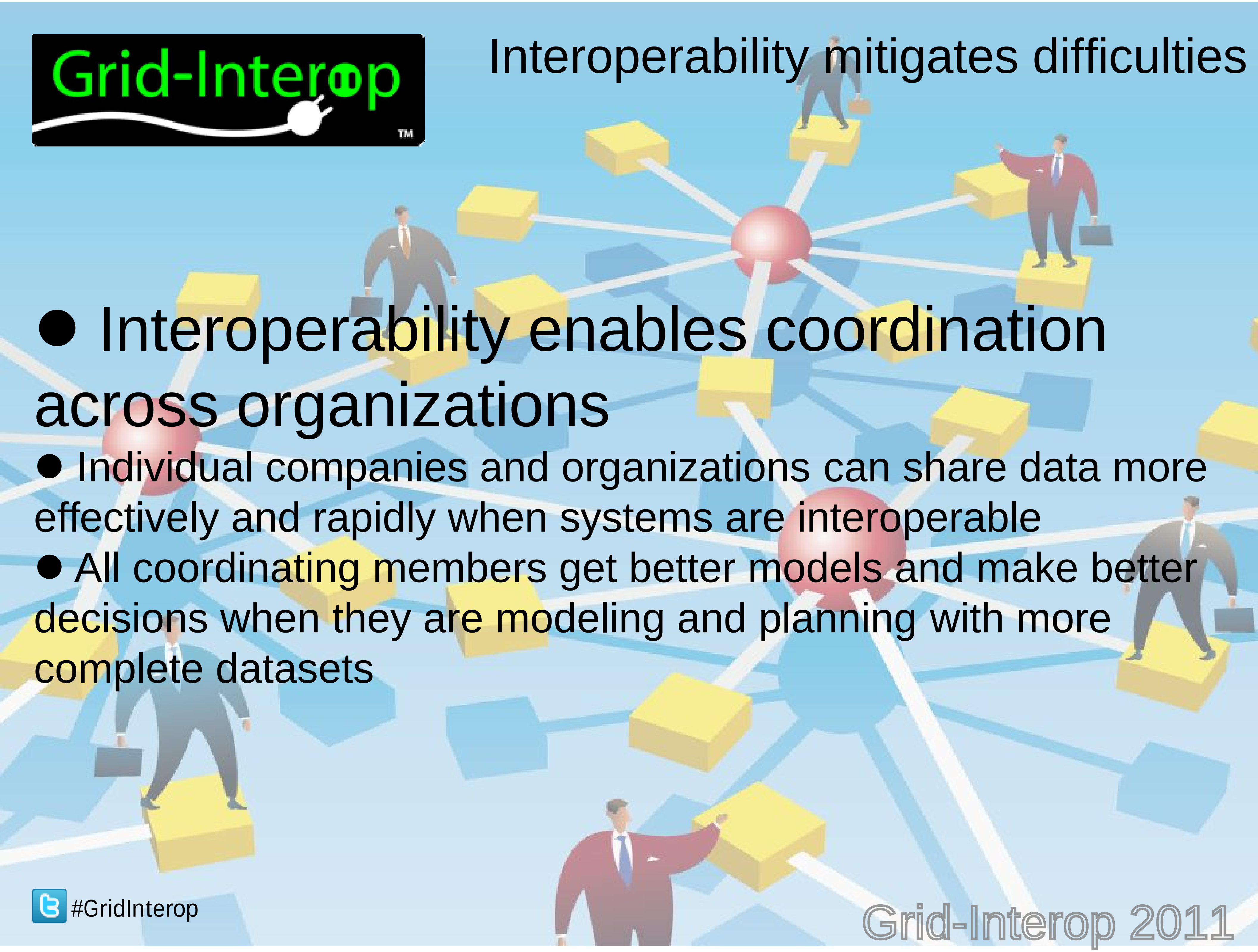
christopher.reed@albeado.com

● Factors that make ROI and CBA difficult

● Lack of substantial historical data within a given company prevents companies from straightforward calculations relating cost and benefits

● Convincing and accurate ROI is difficult to determine when no reduced cost or additional revenues can be calculated or estimated and primary benefit to be derived is avoiding risks and threats that are unfamiliar and of unknown impact

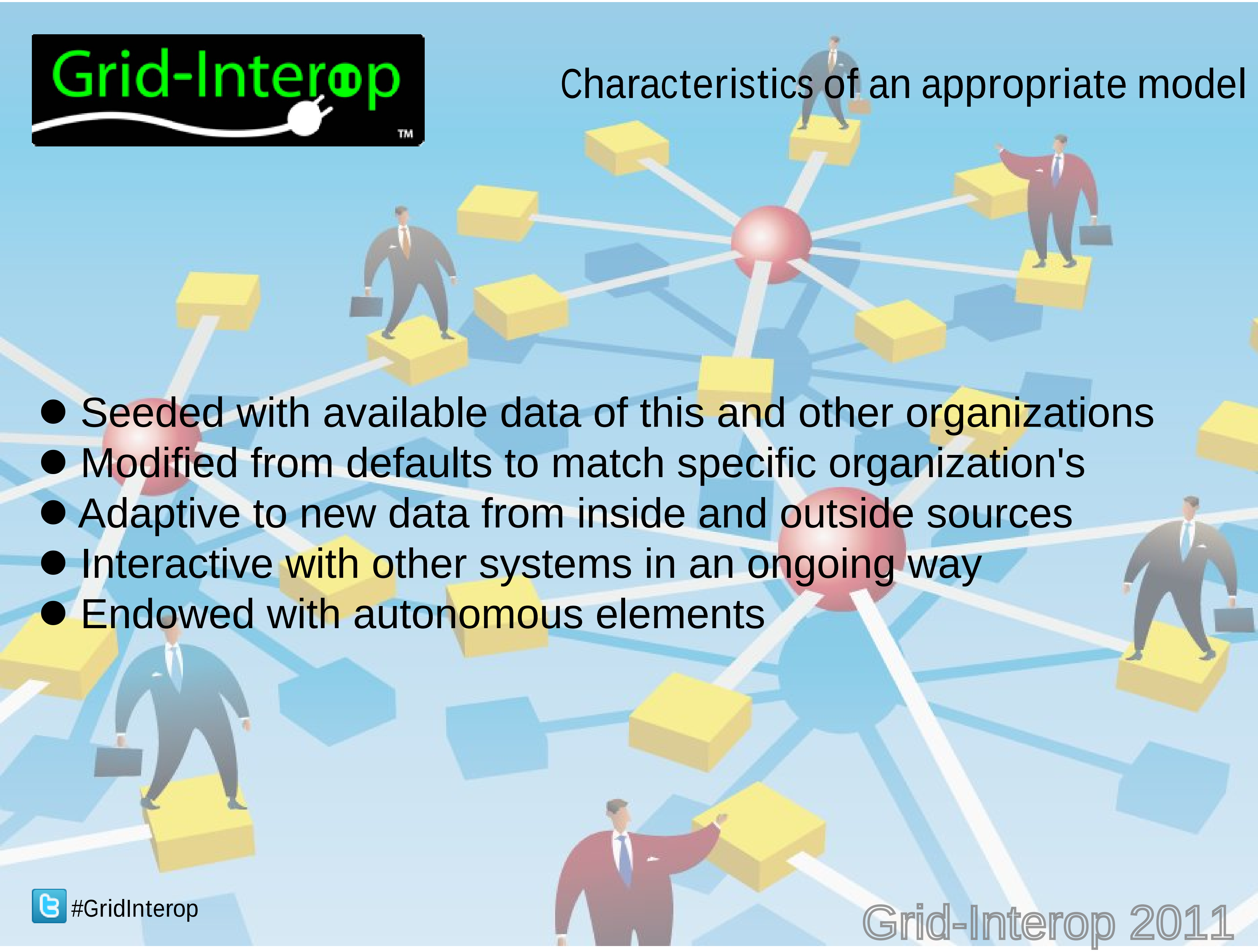
● Those few risks and threats that have produced data are a tiny fraction of those facing the organization



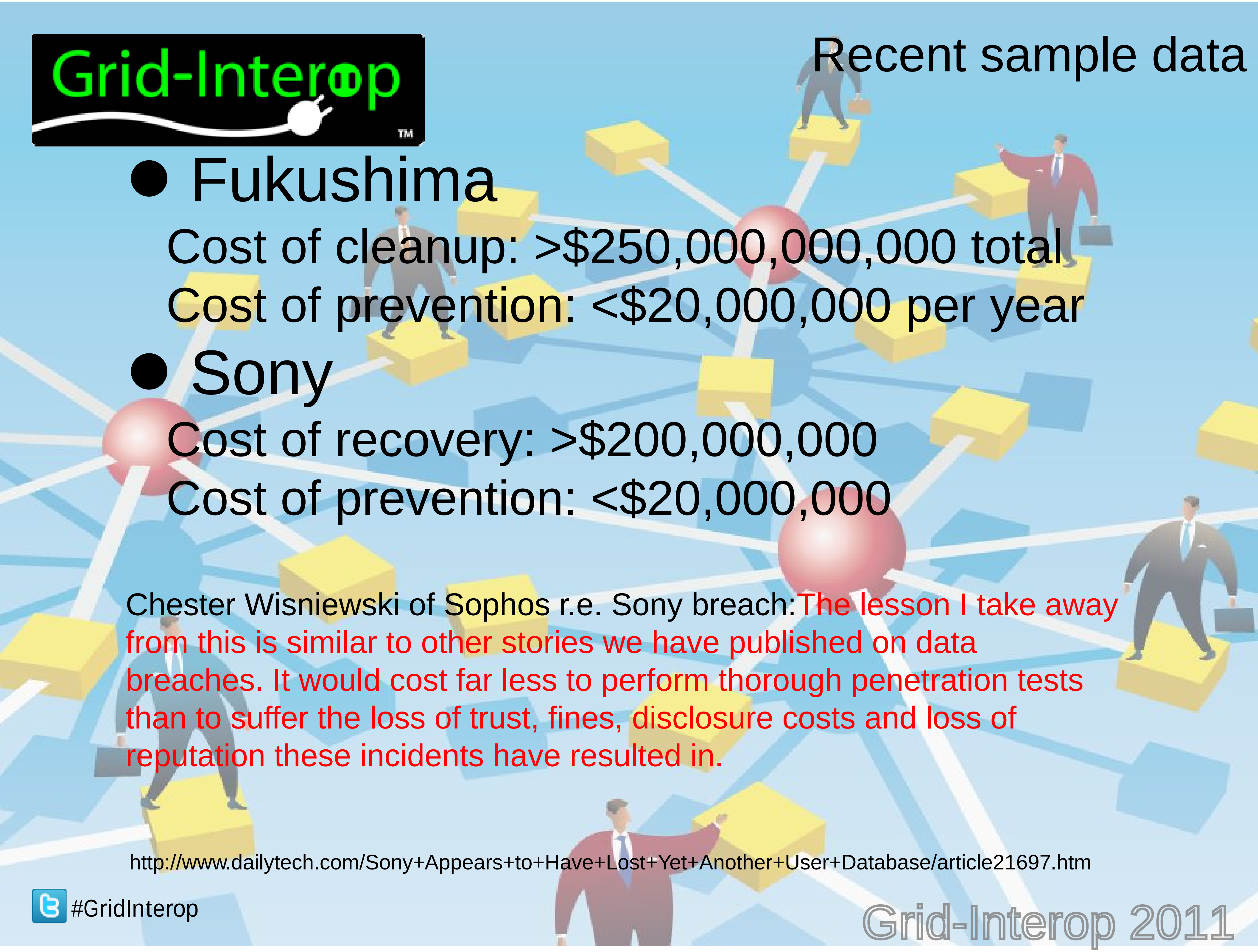
Interoperability mitigates difficulties

- Interoperability enables coordination across organizations
- Individual companies and organizations can share data more effectively and rapidly when systems are interoperable
- All coordinating members get better models and make better decisions when they are modeling and planning with more complete datasets

Characteristics of an appropriate model



- Seeded with available data of this and other organizations
- Modified from defaults to match specific organization's
- Adaptive to new data from inside and outside sources
- Interactive with other systems in an ongoing way
- Endowed with autonomous elements



Recent sample data

- Fukushima

  Cost of cleanup: >$250,000,000,000 total

  Cost of prevention: <$20,000,000 per year

- Sony

  Cost of recovery: >$200,000,000

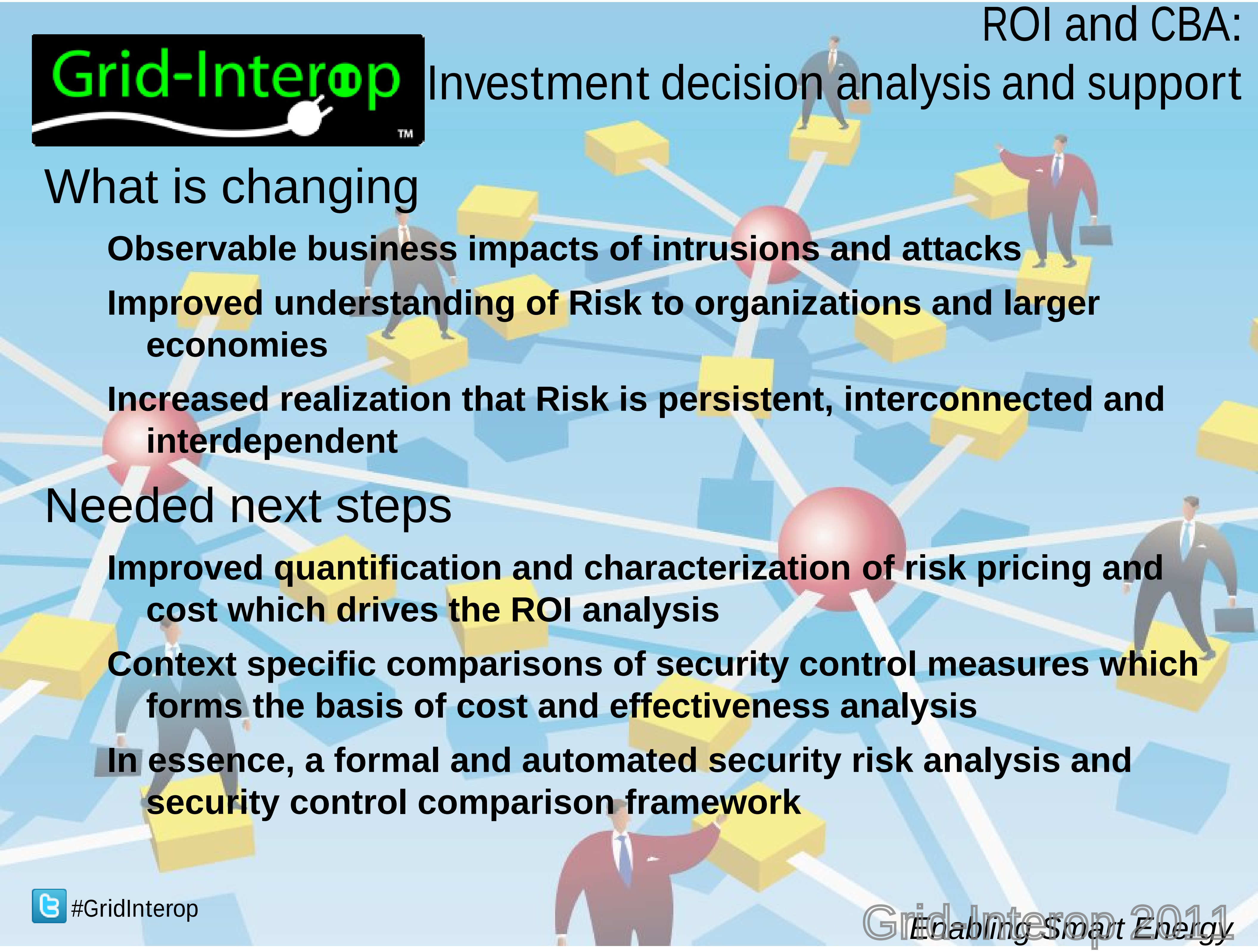
  Cost of prevention: <$20,000,000

Chester Wisniewski of Sophos r.e. Sony breach:The lesson I take away from this is similar to other stories we have published on data breaches. It would cost far less to perform thorough penetration tests than to suffer the loss of trust, fines, disclosure costs and loss of reputation these incidents have resulted in.

http://www.dailytech.com/Sony+Appears+to+Have+Lost+Yet+Another+User+Database/article21697.htm

Security Investment and Cost: Lessons from recent history

- Gaming network intrusion
  - Loss of revenue, assets and information
  - Loss of Customer, public confidence
  - Heightened Regulatory Focus
- Risk Management: concatenated* disasters
  - Largest Utility battling for survival in few months span
  - Economic consequences to the nation is still counting
- Increased deployment and improved technologies for intrusion and attack analysis revealing persistent threats and varied attack motivations



ROI and CBA: Investment decision analysis and support

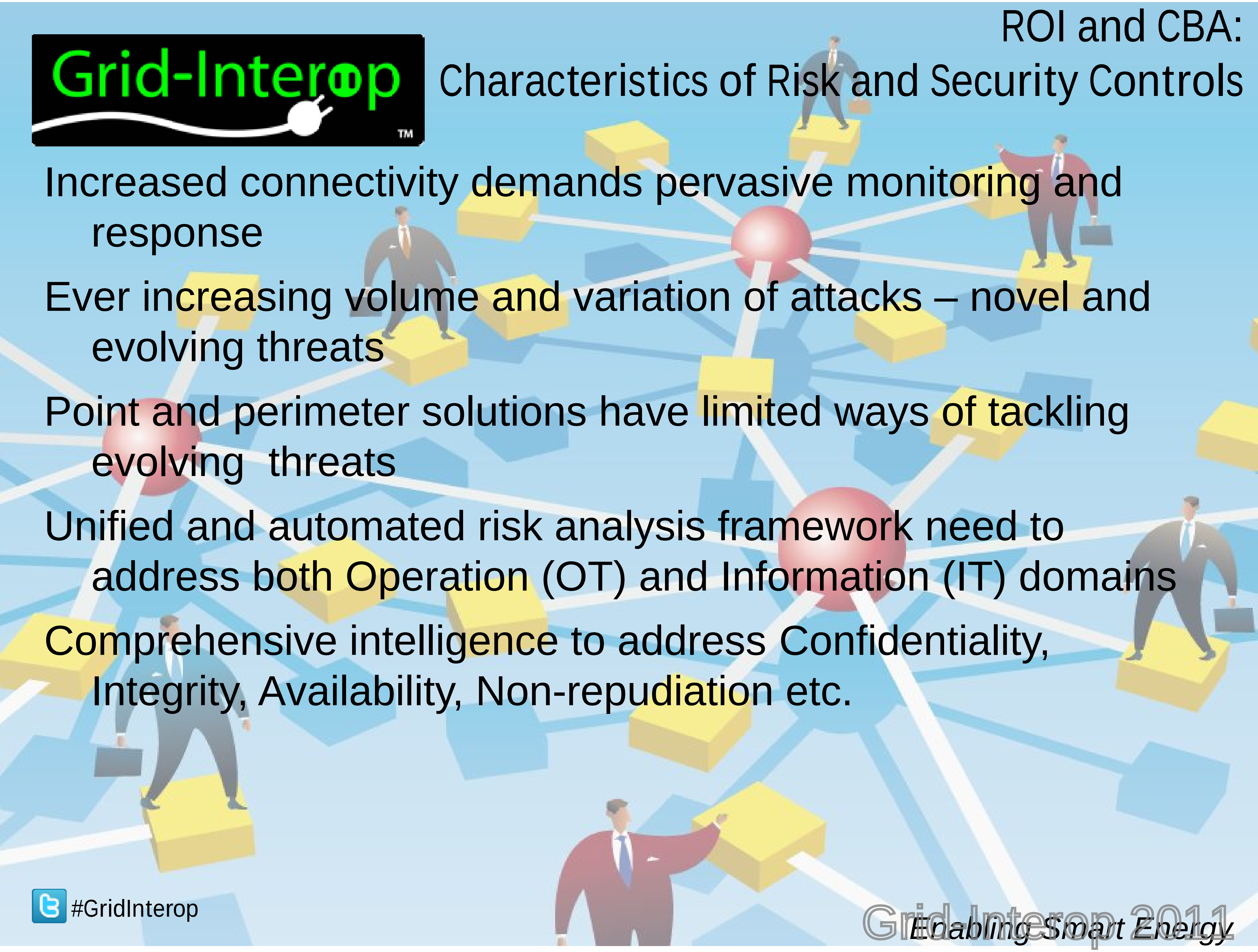
What is changing

- Observable business impacts of intrusions and attacks
- Improved understanding of Risk to organizations and larger economies
- Increased realization that Risk is persistent, interconnected and interdependent

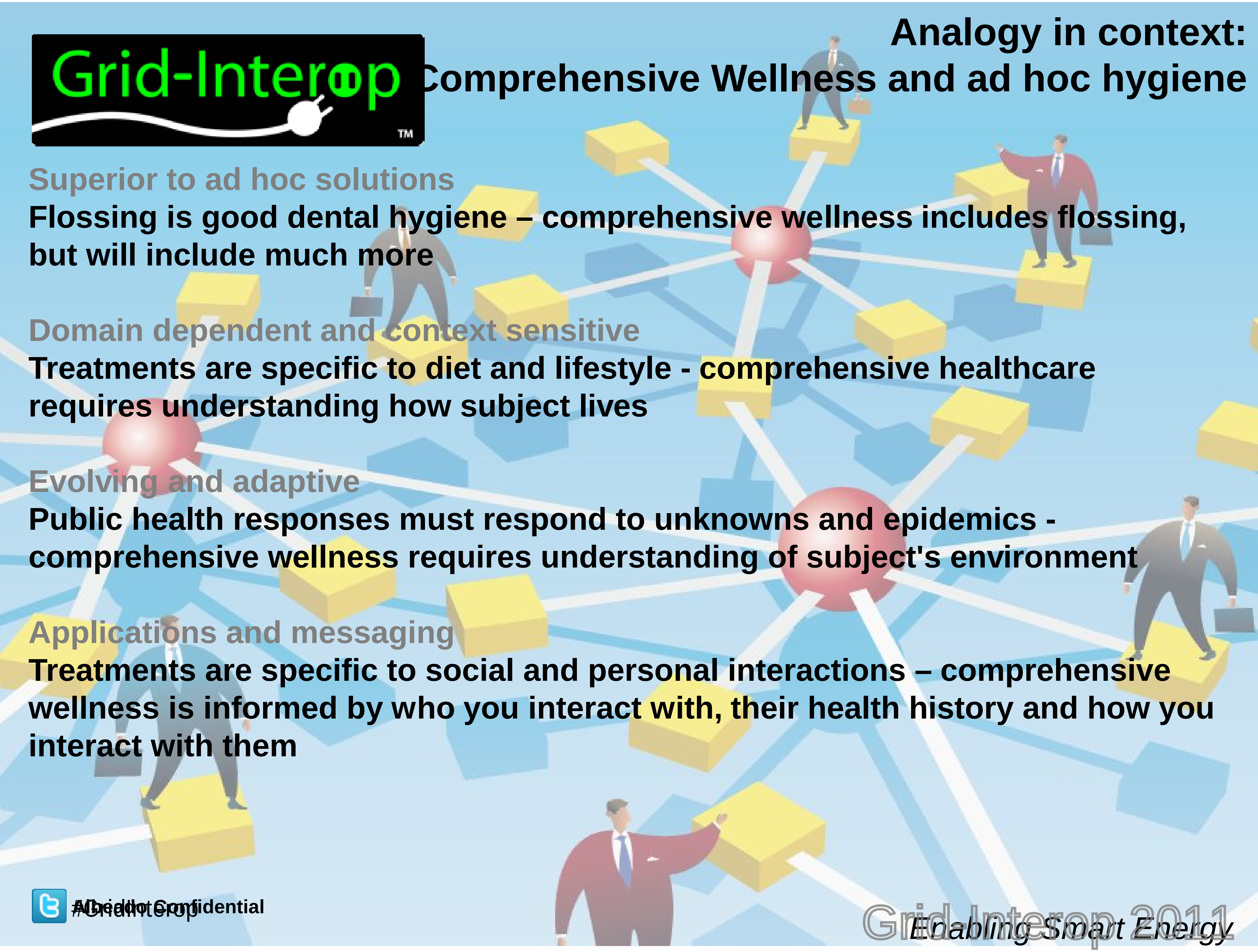
Needed next steps

- Improved quantification and characterization of risk pricing and cost which drives the ROI analysis
- Context specific comparisons of security control measures which forms the basis of cost and effectiveness analysis
- In essence, a formal and automated security risk analysis and security control comparison framework

ROI and CBA:
Characteristics of Risk and Security Controls



- Increased connectivity demands pervasive monitoring and response
- Ever increasing volume and variation of attacks – novel and evolving threats
- Point and perimeter solutions have limited ways of tackling evolving threats
- Unified and automated risk analysis framework need to address both Operation (OT) and Information (IT) domains
- Comprehensive intelligence to address Confidentiality, Integrity, Availability, Non-repudiation etc.



Analogy in context: Comprehensive Wellness and ad hoc hygiene

Superior to ad hoc solutions

Flossing is good dental hygiene – comprehensive wellness includes flossing, but will include much more

Domain dependent and context sensitive

Treatments are specific to diet and lifestyle - comprehensive healthcare requires understanding how subject lives

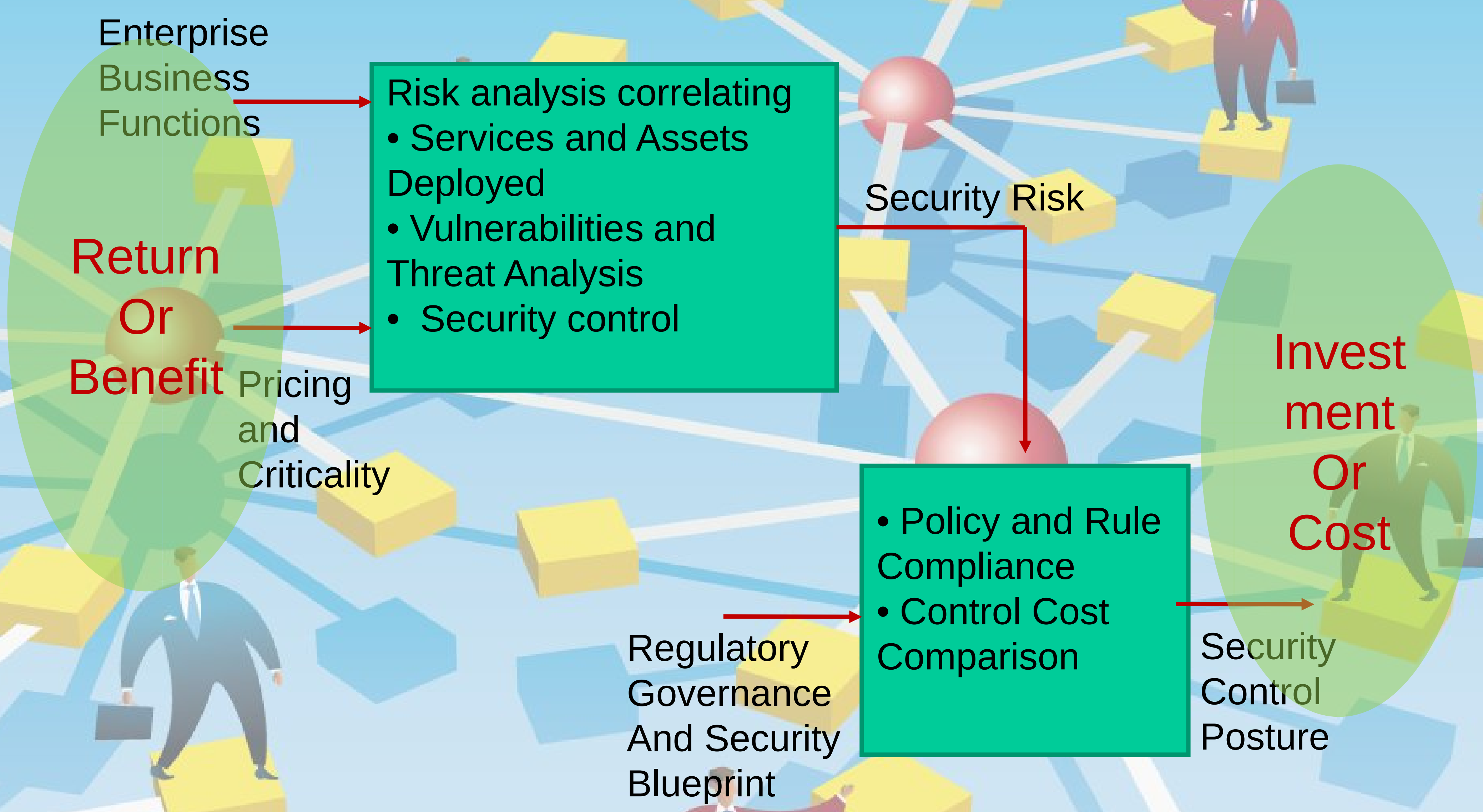
Evolving and adaptive

Public health responses must respond to unknowns and epidemics - comprehensive wellness requires understanding of subject's environment

Applications and messaging

Treatments are specific to social and personal interactions – comprehensive wellness is informed by who you interact with, their health history and how you interact with them

Security Risk: ROI and CBA Decision Support



Enterprise Business Functions

Return Or Benefit

Pricing and Criticality

Risk analysis correlating
- Services and Assets Deployed
- Vulnerabilities and Threat Analysis
- Security control

Security Risk

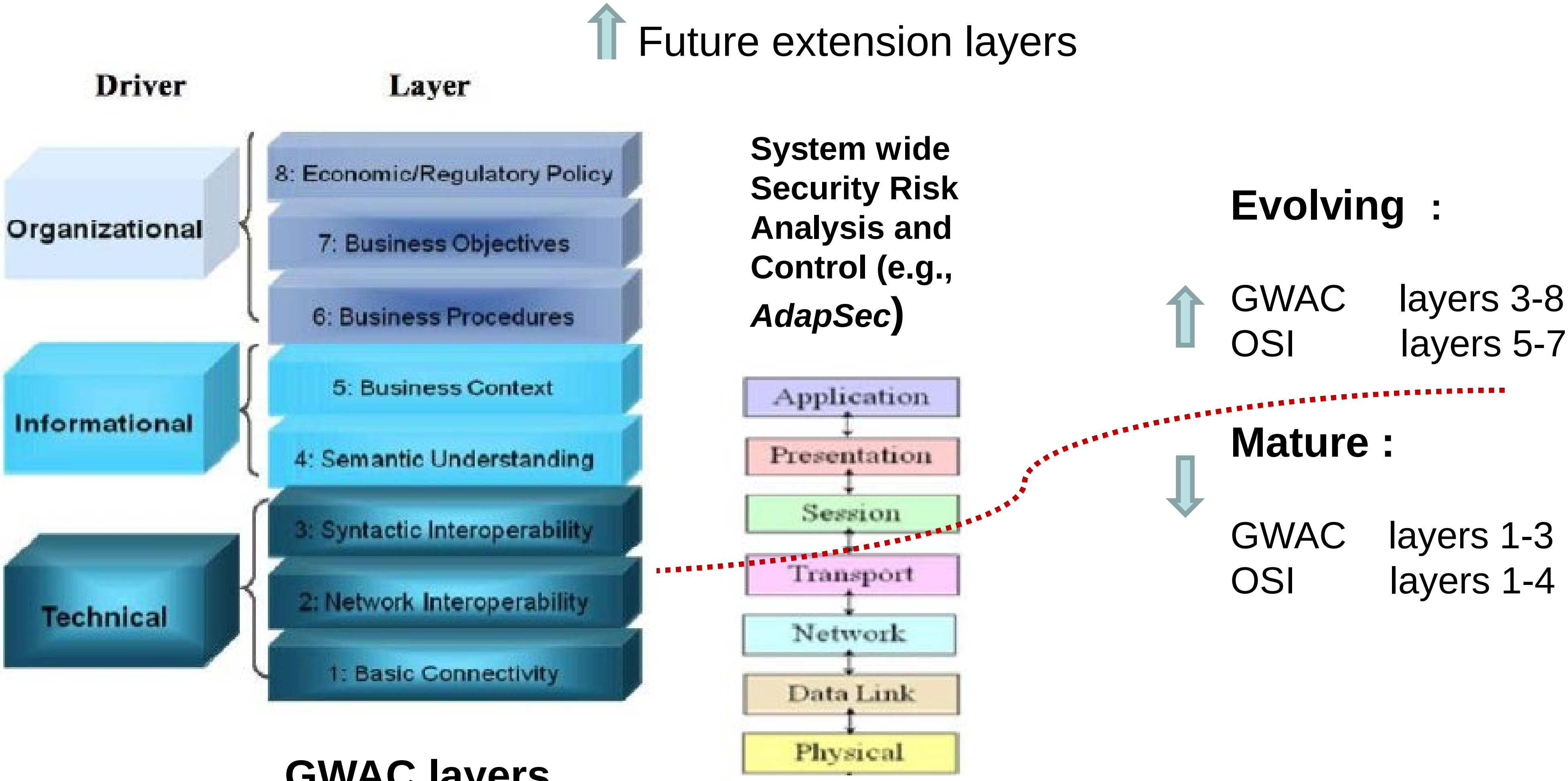
- Policy and Rule Compliance
- Control Cost Comparison

Regulatory Governance And Security Blueprint

Security Control Posture

Investment Or Cost

GWAC and OSI: Experience in Interoperability



System wide Security Risk Analysis and Control (e.g., *AdapSec*)

Evolving :

GWAC	layers 3-8
OSI	layers 5-7

Mature :

GWAC	layers 1-3
OSI	layers 1-4

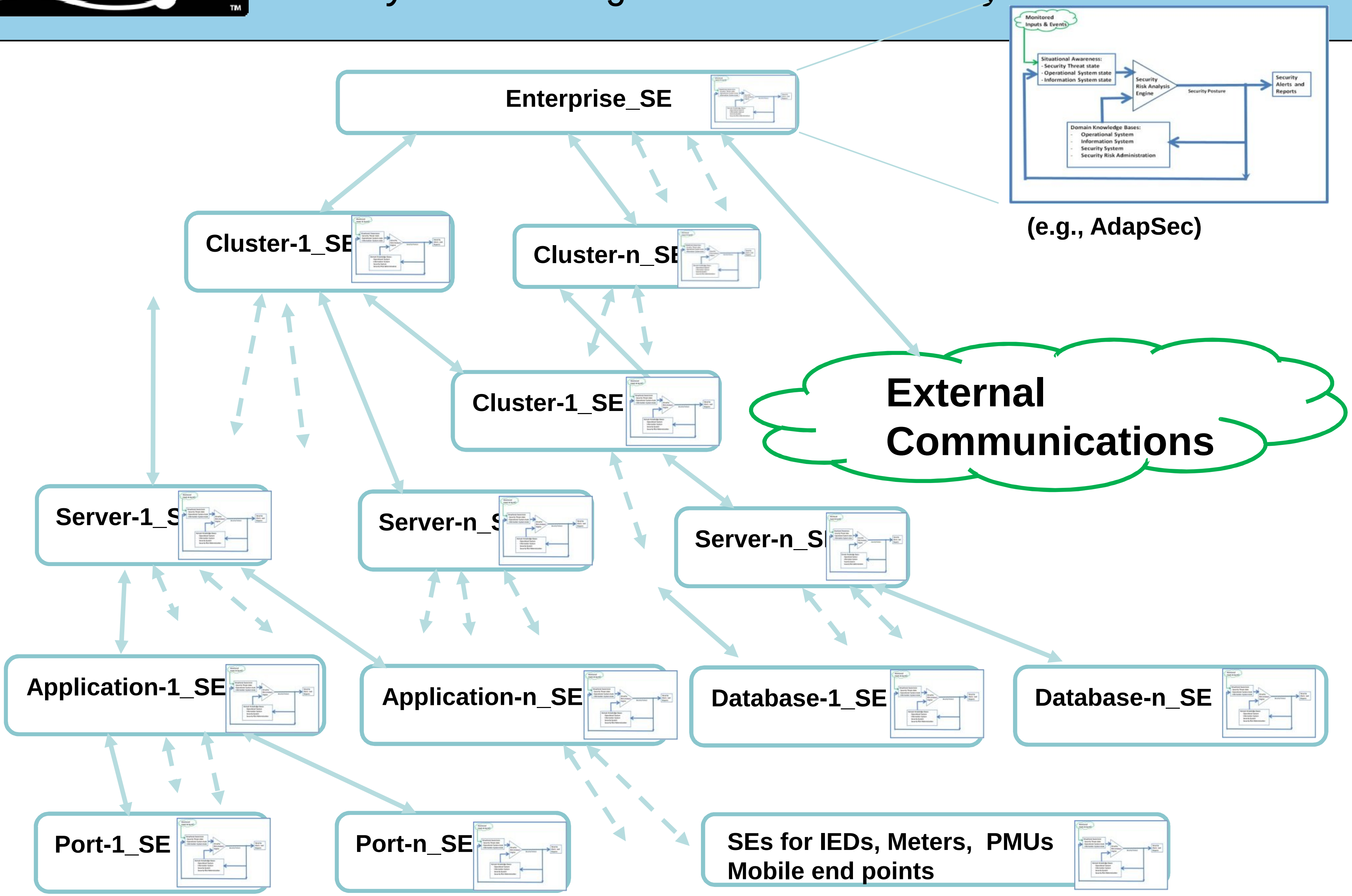
GWAC layers

OSI layers

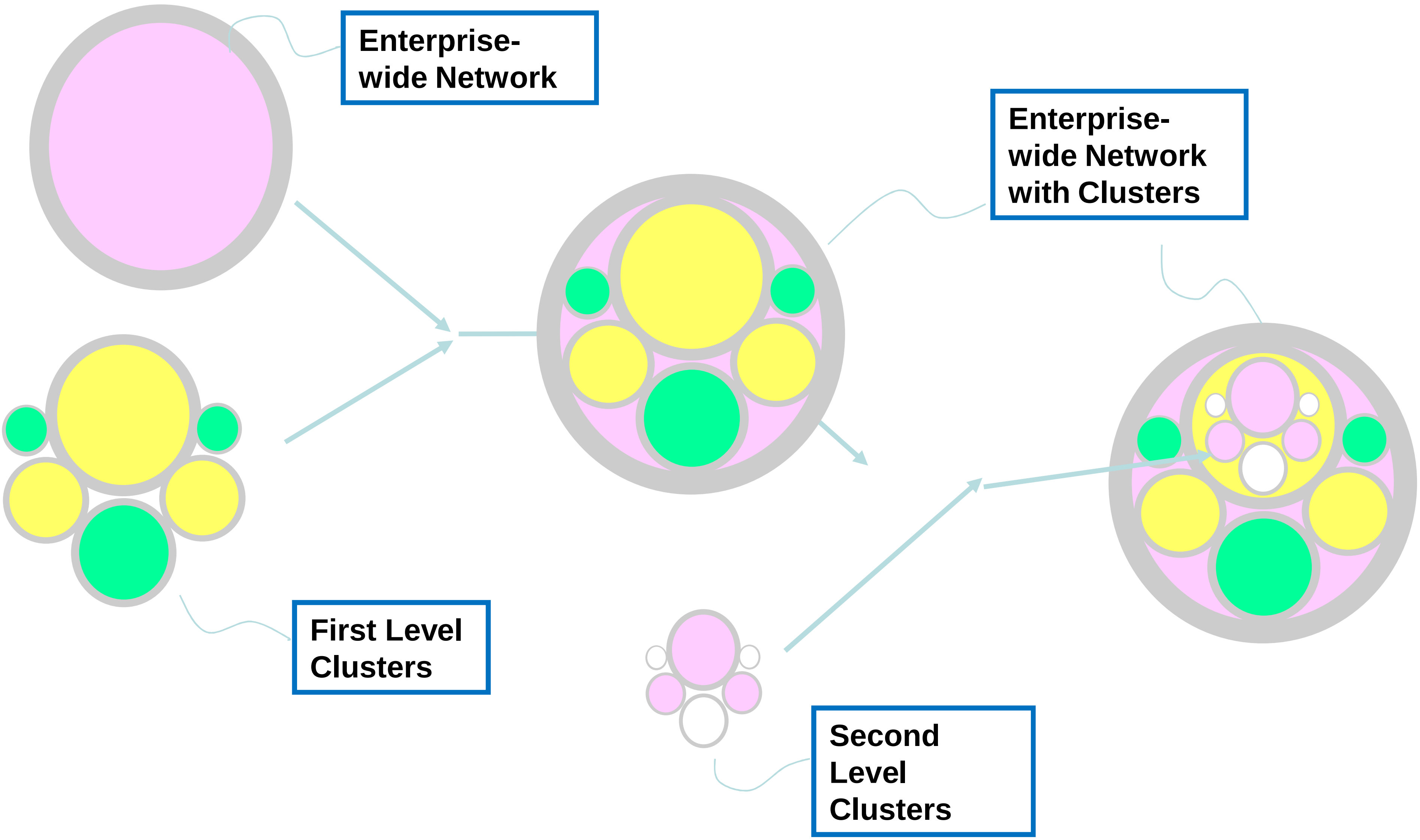
Layering enhances interoperability

Grid-Interop™

Enterprise Wide Interoperability: Security Monitoring & Control Hierarchy



Composition of Self-Similar Interoperating Clusters: Making of Enterprise Wide Network



Enterprise-wide Network

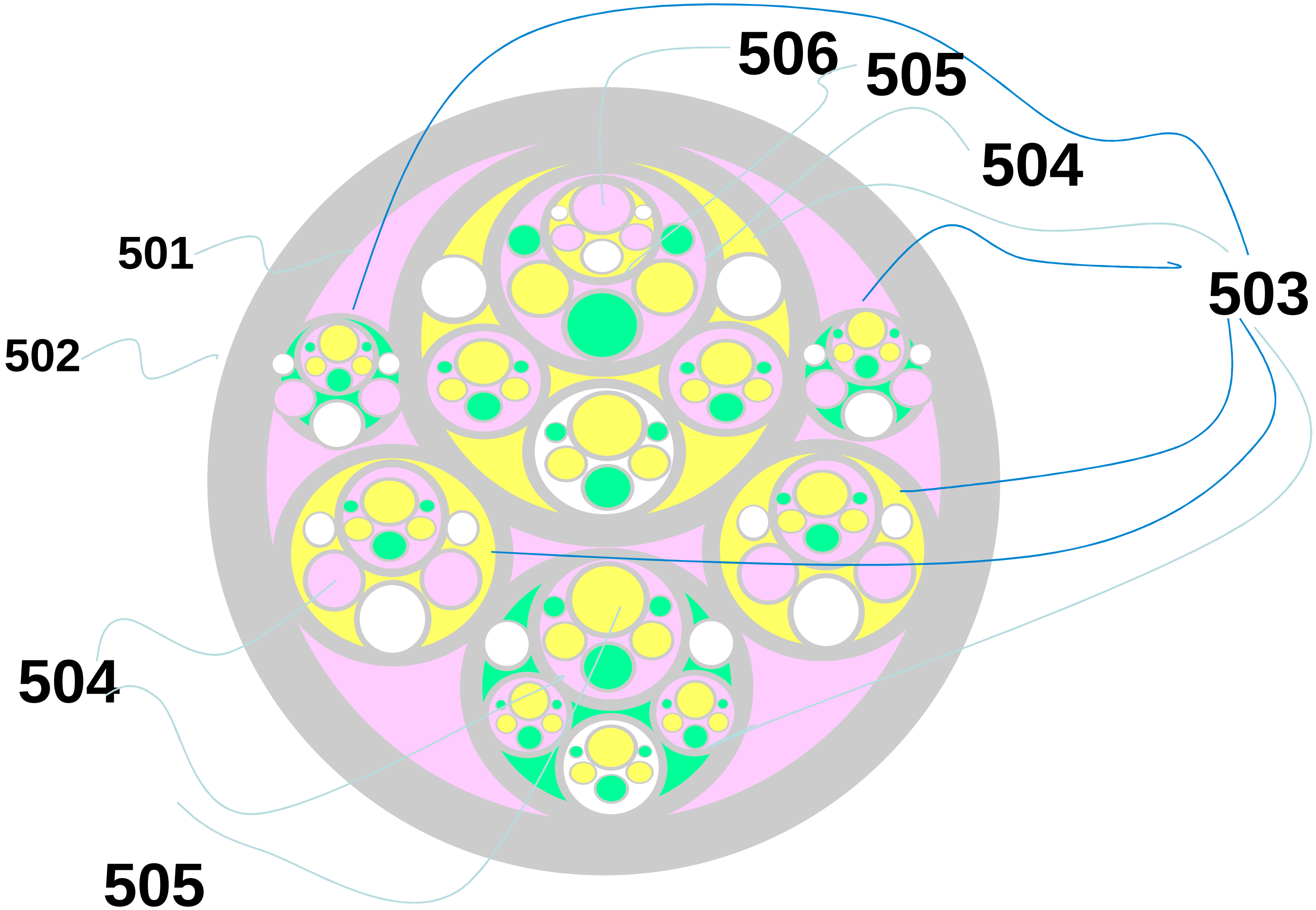
First Level Clusters

Enterprise-wide Network with Clusters

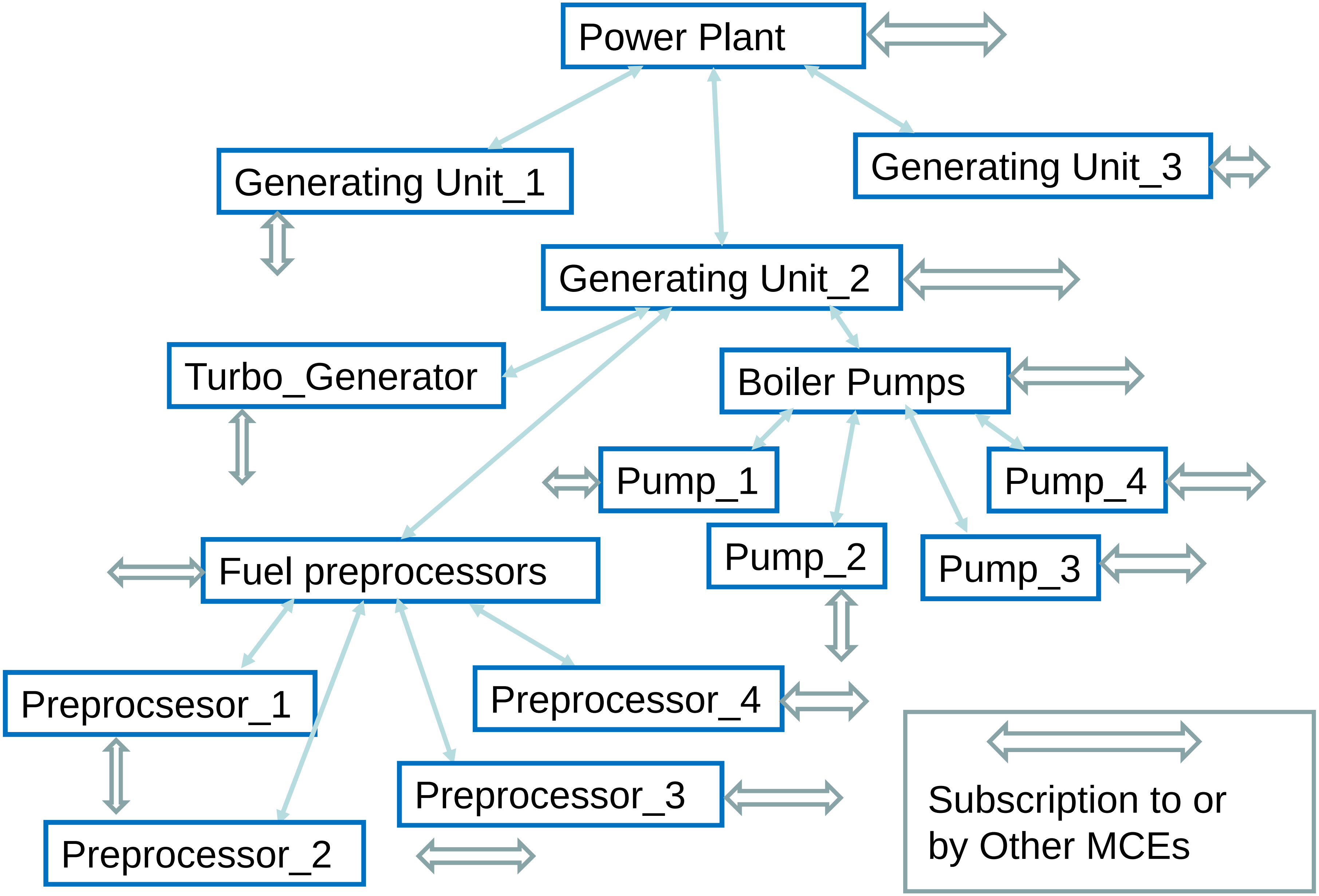
Second Level Clusters

Grid-Interop

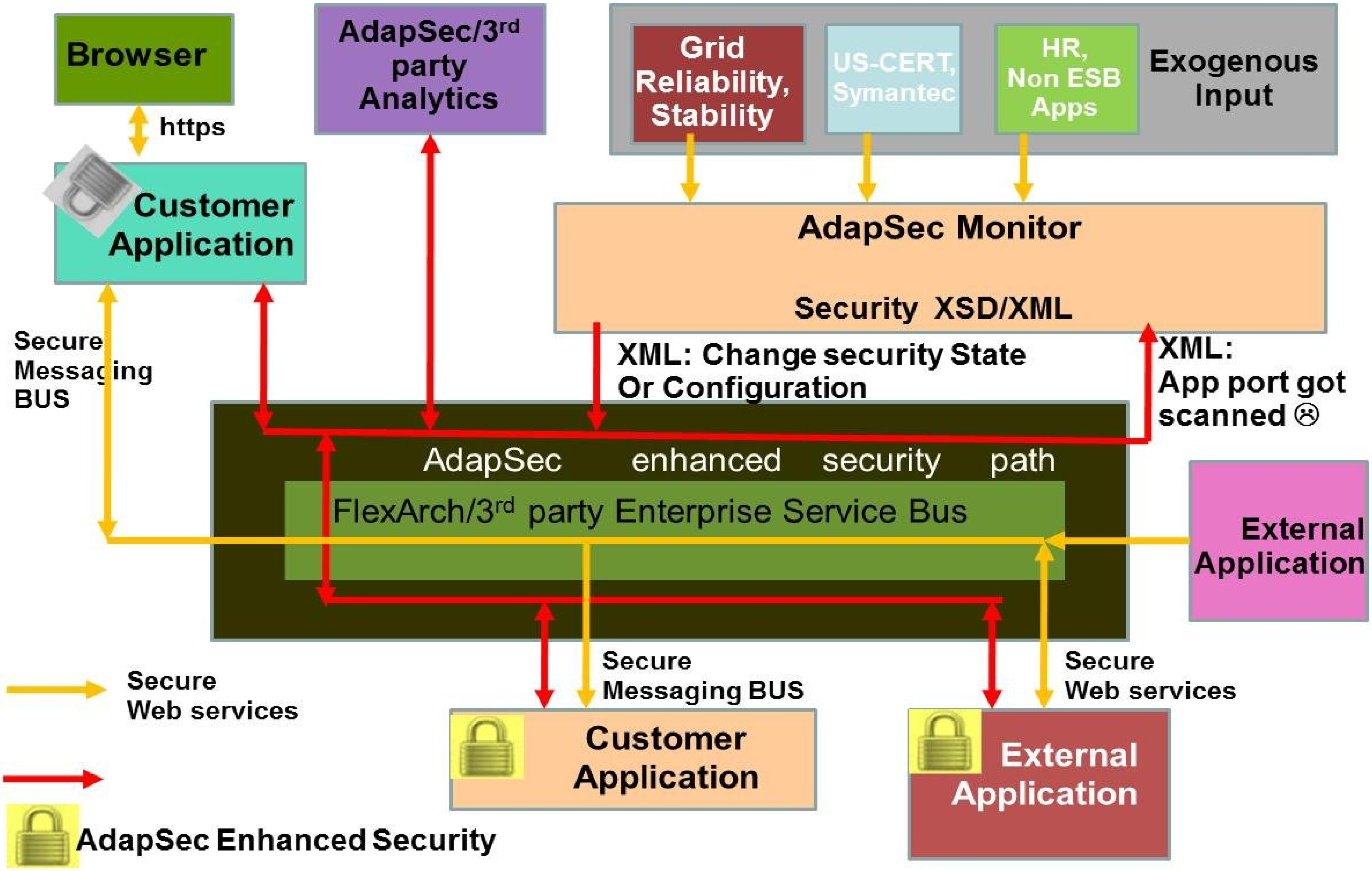
Functionally Pervasive, Structurally Self-similar



Pervasively distributed and coordinated Analysis and Control Environment



Pervasive Message and Application Security: Role of Interoperability



Browser

https

Customer Application

AdapSec/3rd party Analytics

Grid Reliability, Stability

US-CERT, Symantec

HR, Non ESB Apps

Exogenous Input

AdapSec Monitor

Security XSD/XML

XML: Change security State Or Configuration

XML: App port got scanned ☹

Secure Messaging BUS

AdapSec enhanced security path

FlexArch/3rd party Enterprise Service Bus

External Application

Secure Messaging BUS

Secure Web services

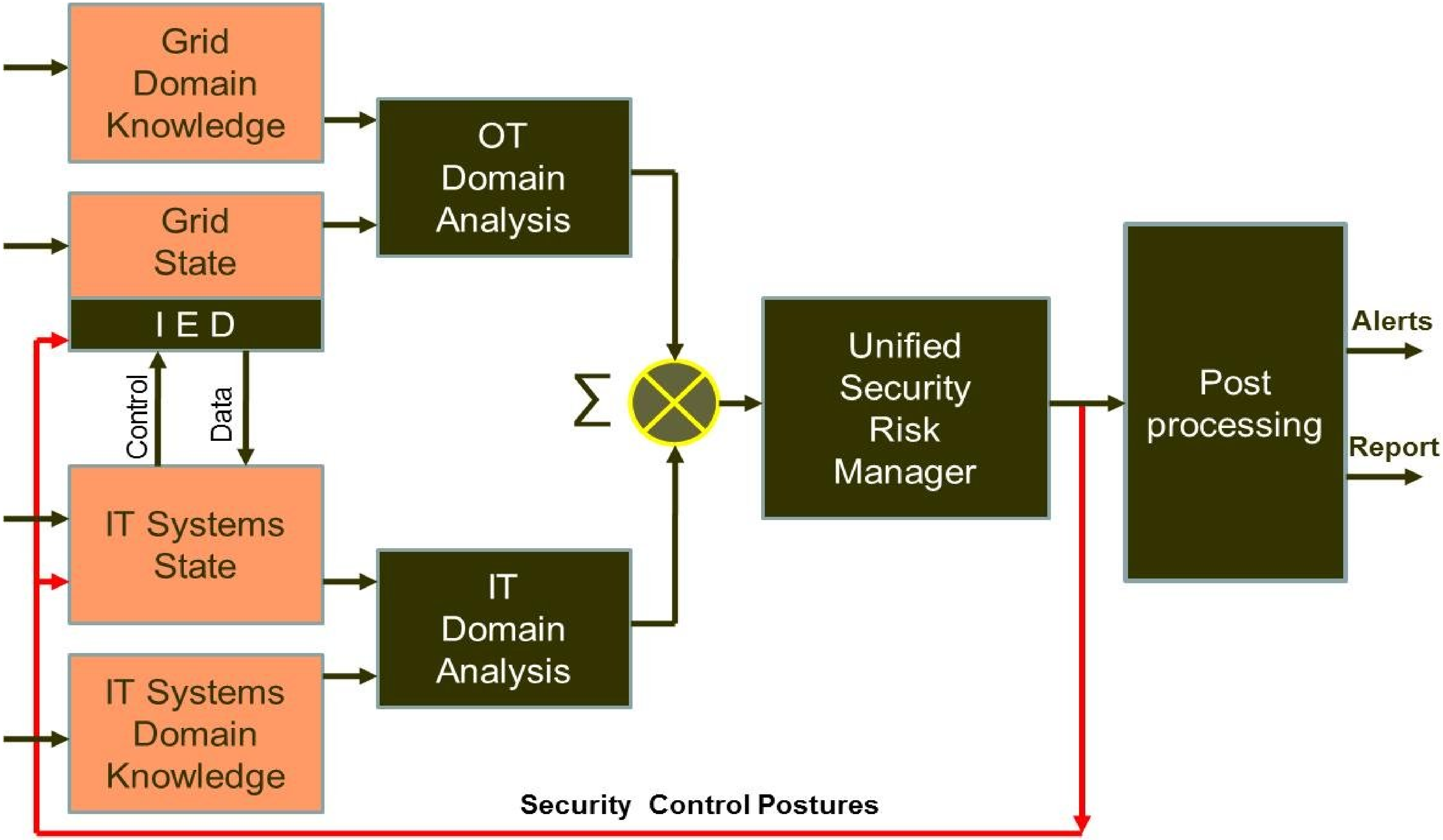
Customer Application

External Application

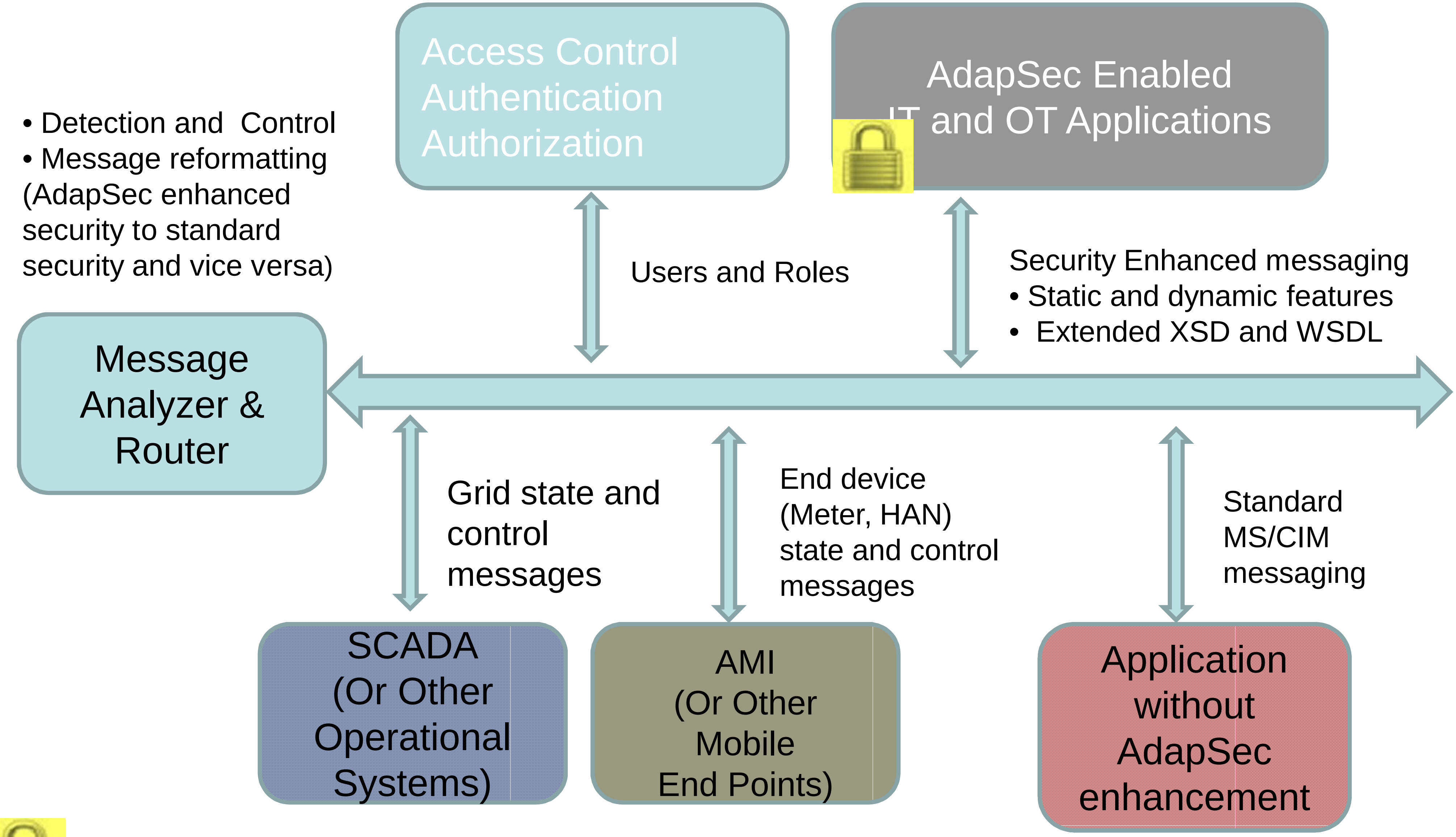
Secure Web services

AdapSec Enhanced Security

Unified and Adaptive OT and IT Domain Aware Security: Interoperability of data and protocol



Adaptive security: Interoperable components



- Detection and Control
- Message reformatting (AdapSec enhanced security to standard security and vice versa)

Access Control
Authentication
Authorization

AdapSec Enabled
IT and OT Applications

Users and Roles

Security Enhanced messaging
- Static and dynamic features
- Extended XSD and WSDL

Message Analyzer & Router

Grid state and control messages

End device (Meter, HAN) state and control messages

Standard MS/CIM messaging

SCADA
(Or Other Operational Systems)

AMI
(Or Other Mobile
End Points)

Application without AdapSec enhancement

🔒 **AdapSec Enhanced Security**

END