METERING INTERNATIONAL | SMARTENERGY CANADA

Update On Smart Grid Cyber Security

Kshamit Dixit
Manager – IT Security,
Toronto Hydro ,
Ontario, Canada

toronto hydro corporation

Agenda

- Cyber Security Overview
- Security Framework
- Securing Smart Grid

Smart Grid Attack Threats

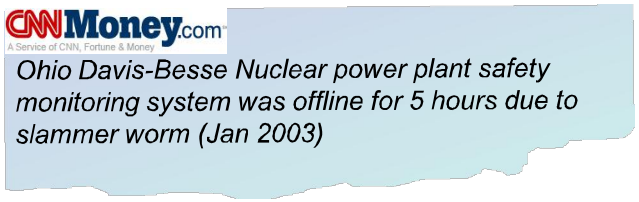
"Energy control systems are subject to targeted cyber attacks. Potential adversaries have pursued progressively devious means to exploit flaws in system components, telecommunication methods, and common operating systems found in modern energy systems with the intent to infiltrate and sabotage vulnerable control systems."

"Sophisticated cyber attack tools require little technical knowledge to use and can be found on the Internet, as can manufacturers' technical specifications for popular control system equipment."

Source: Roadmap to Secure Control Systems in the Energy Sector, The Department of Homeland Security and US Department of Energy

Critical Infrastructure Security Challenges

- **Cyber attacks can change every 30-60 seconds**
  - Requires integrated, quick response system.
- **Convergence of traditionally isolated control systems**
  - Cyber vulnerabilities introduced to critical systems
  - Mitigation strategies not as easy as regular IT
- **Utilities tend to work internally in silos**
  - Prevents rapid exchange of identity information between different departments



The Landscape is Changing Around Us

"We have information, from multiple regions outside the United States, of cyber intrusions into utilities, followed by extortion demands…"

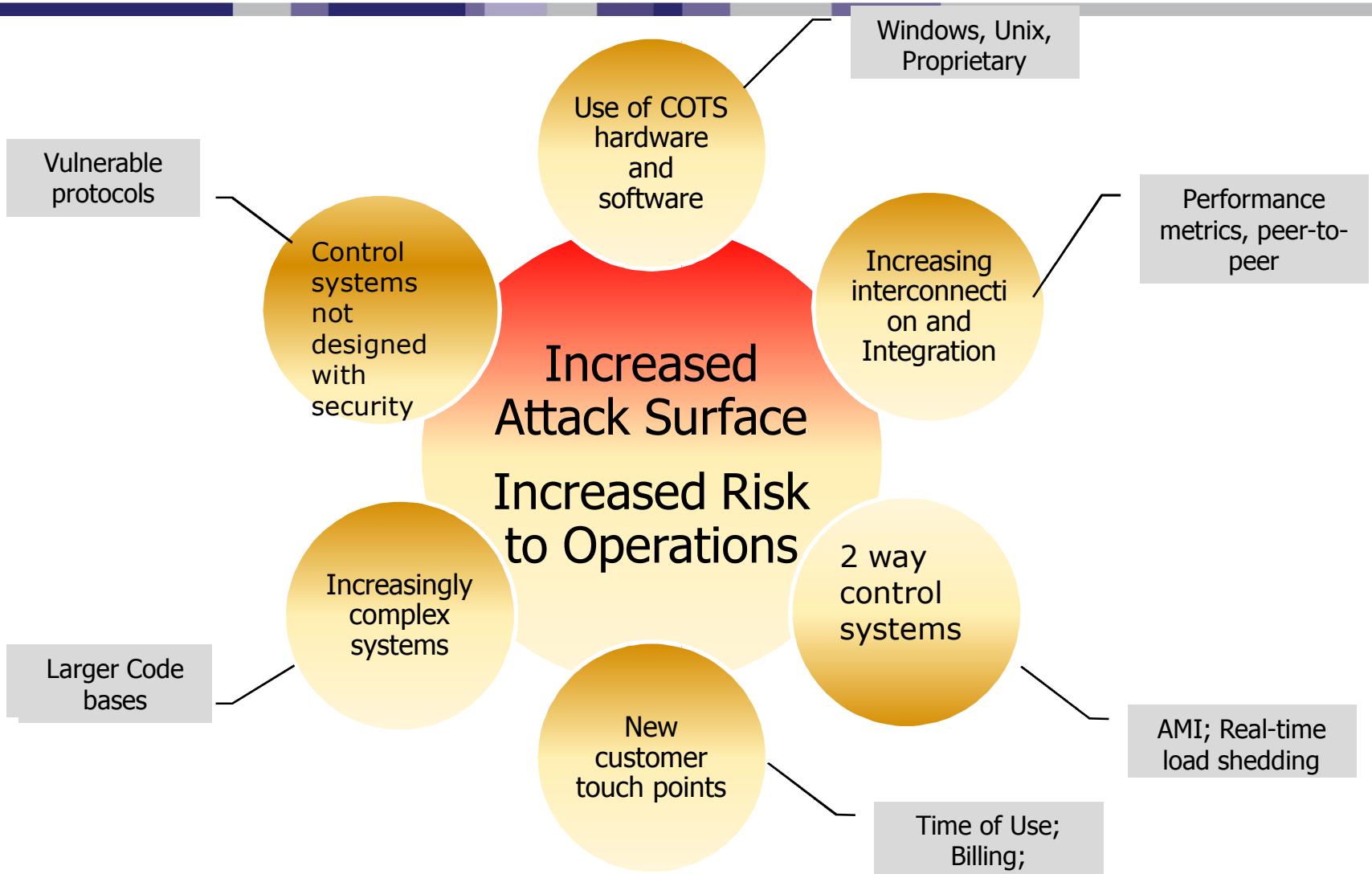
"…We have information that cyber attacks have been used to disrupt power equipment in several regions outside the United States. In at least one case, the disruption caused a power outage affecting multiple cities."

"We do not know who executed these attacks or why, but all involved intrusions through the Internet."

Central Intelligence Agency, 2008

<u>Did this include any Smart Grid elements???</u>

Cyber Security Drivers



Access Points: Numerous and Diverse

- Due to convergence, the number of access points has increased:
  - Access from the Internet
  - Access from corporate users
  - Access into SCADA LAN (keep operators happy)
  - Access from the vendors
  - Access from the upstream providers
- Metering system connects directly to corporate in many cases
  - Customer care and billing requires maximum integrity
  - Methods for communications is in open source
- Defense in depth is the only real countermeasure
  - Zones
  - Conduits
  - Layered defense modeling
  - Unified Threat Management and Anomaly Detection

Emerging Issues

- Current Smart Grid/Meter solution is prescriptive for only one-way control traffic
  - But what about meters deployed with 'kill switch' enabled?
  - California PCT program can provide a tremendous foundation
- Future will migrate to 802.x communications
  - How will THAT be secured?
  - 802.15.4 proven to vulnerable to jamming (Jan 2009)
  - How much more vulnerable will the system be?
- What can the vendor do to ensure security of Grid operation
  - Proof of concept to get security keys from chipset (Feb 2009)
  - Mobile worm can impact firmware in all meters in mesh grid (because it is 'smart')
- What can the utility do to protect metering?
  - More than simple IDS deployed to the meter level – must include defining operational envelope
  - Security Information and Event Monitoring (SIEM) must be cost effective, scalable, AND non-intrusive to collection operations

Question – How is Security Being Done?

- Has anyone looked into the cyber security issues of the Smart Meter system and Smart Grid?
  - Yes, and it is not pretty
- How do we protect the control of the meters, our grid and the customer data?
  - Delicate balance required
- How can cyber security be a value-add to the customer?
  - Meters and SG must communicate reliably AND securely to central location. But how do we enforce the mechanisms? (cell, analog, 802.x, BPL)

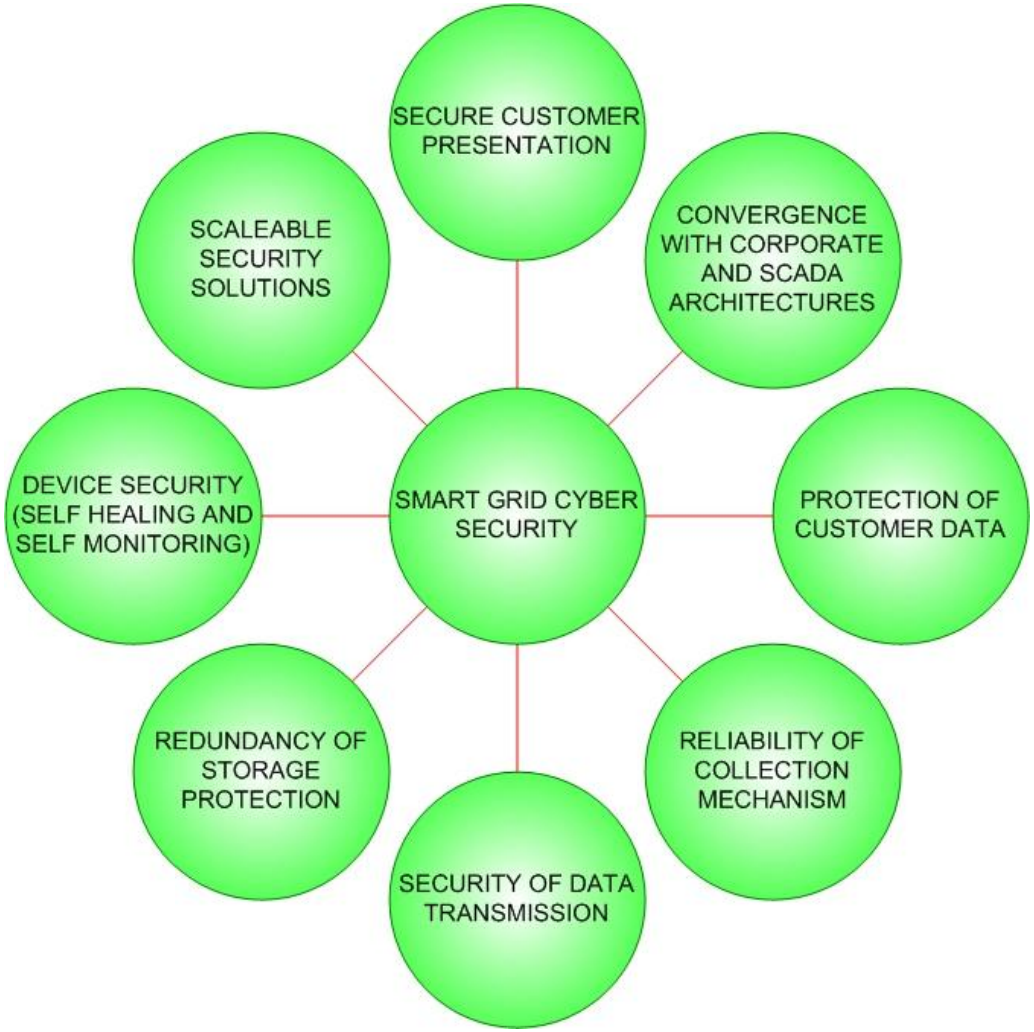
Current and Future Scenario

20th Century Grid	21st Century Smart Grid
Electromechanical	Digital
One-way communication (if any)	Two-way communication
Built for centralized generation	Accommodates distributed generation
Radial topology	Network topology
Few sensors	Monitors and sensors throughout
“Blind”	Self-monitoring
Manual restoration	Semi-automated restoration, and eventually self-healing
Prone to failures and blackouts	Adaptive protection and islanding
Check equipment manually	Monitor equipment remotely
Emergency decisions by committee and phone	Decision support systems, predictive reliability
Limited control over power flows	Pervasive control systems
Limited price information	Full price information
Few customer choices	Many customer choices

Source: The Emerging Smart Grid

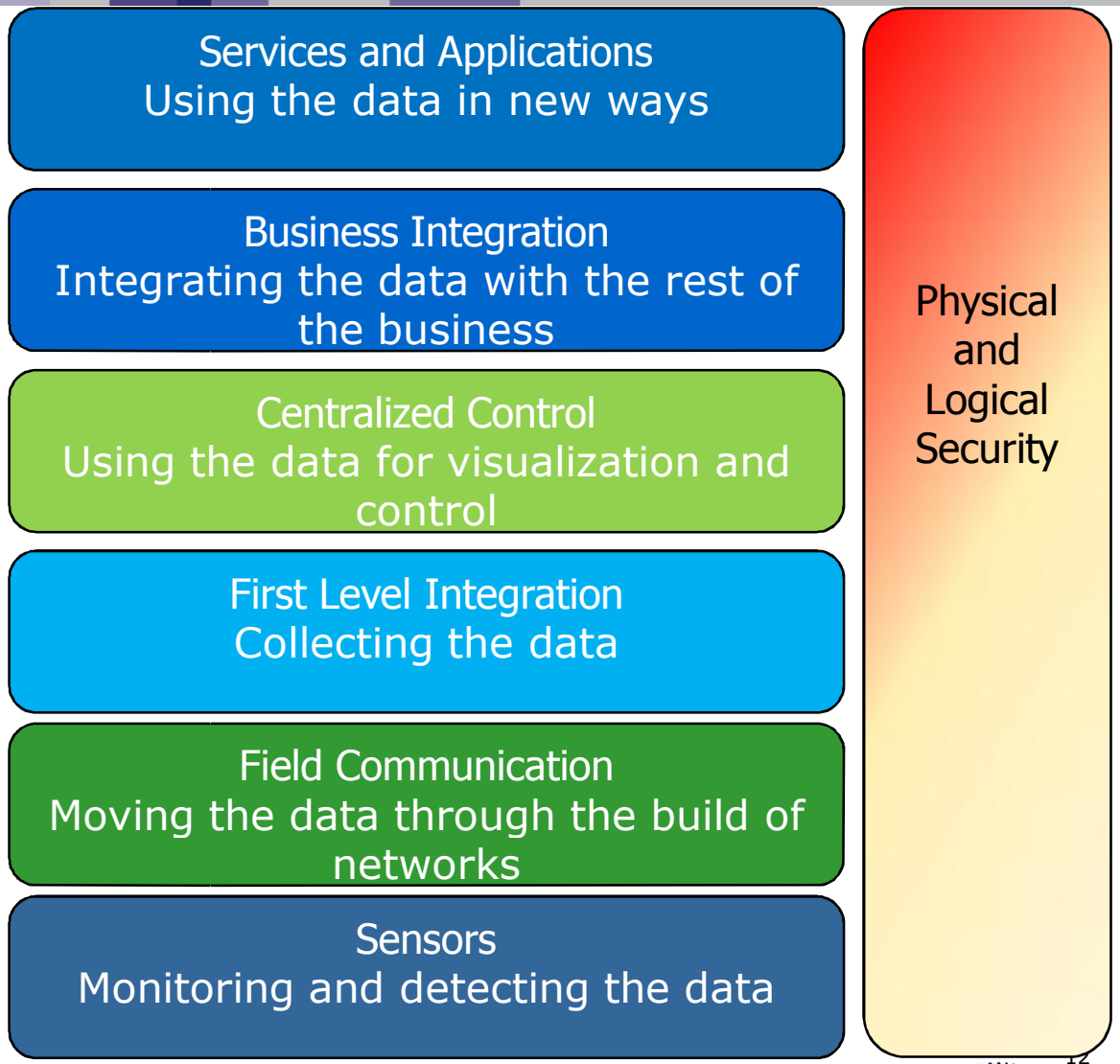
Current Issues in Smart Grid Cyber Security

- Need to protect Time of Use (TOU) data and access from non-authorized users
- Need to protect meters from being abused as control channel into grid operations
- Need to protect future two-way communications for meter activity
- Need to ensure future control capability is secure



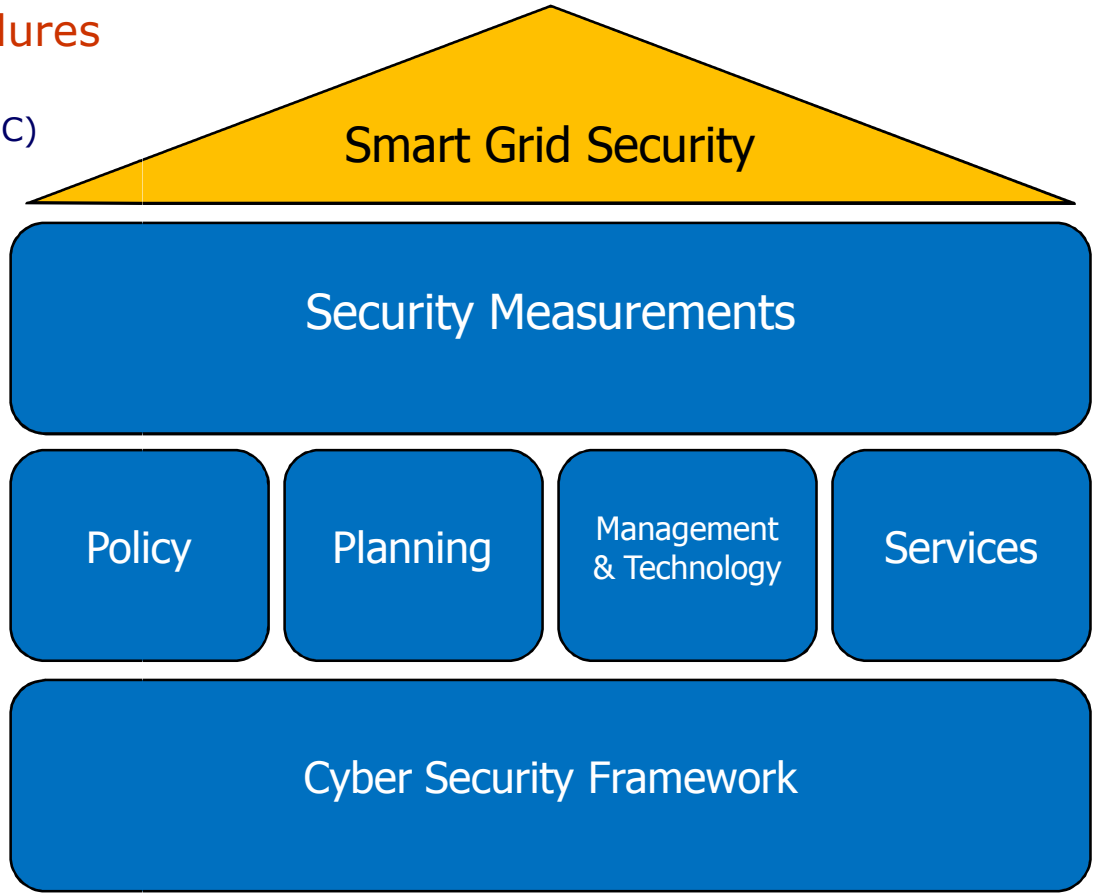
Smart Grid Characteristics ,Technology & Security

- Self-healing
- Empowers and incorporates the consumer
- Resilient to physical and cyber attacks
- Provides power quality needed by 21st century users
- Accommodates a wide variety of generation options
- Fully enables maturing electricity markets
- Optimizes assets



Smart Grid Security Components

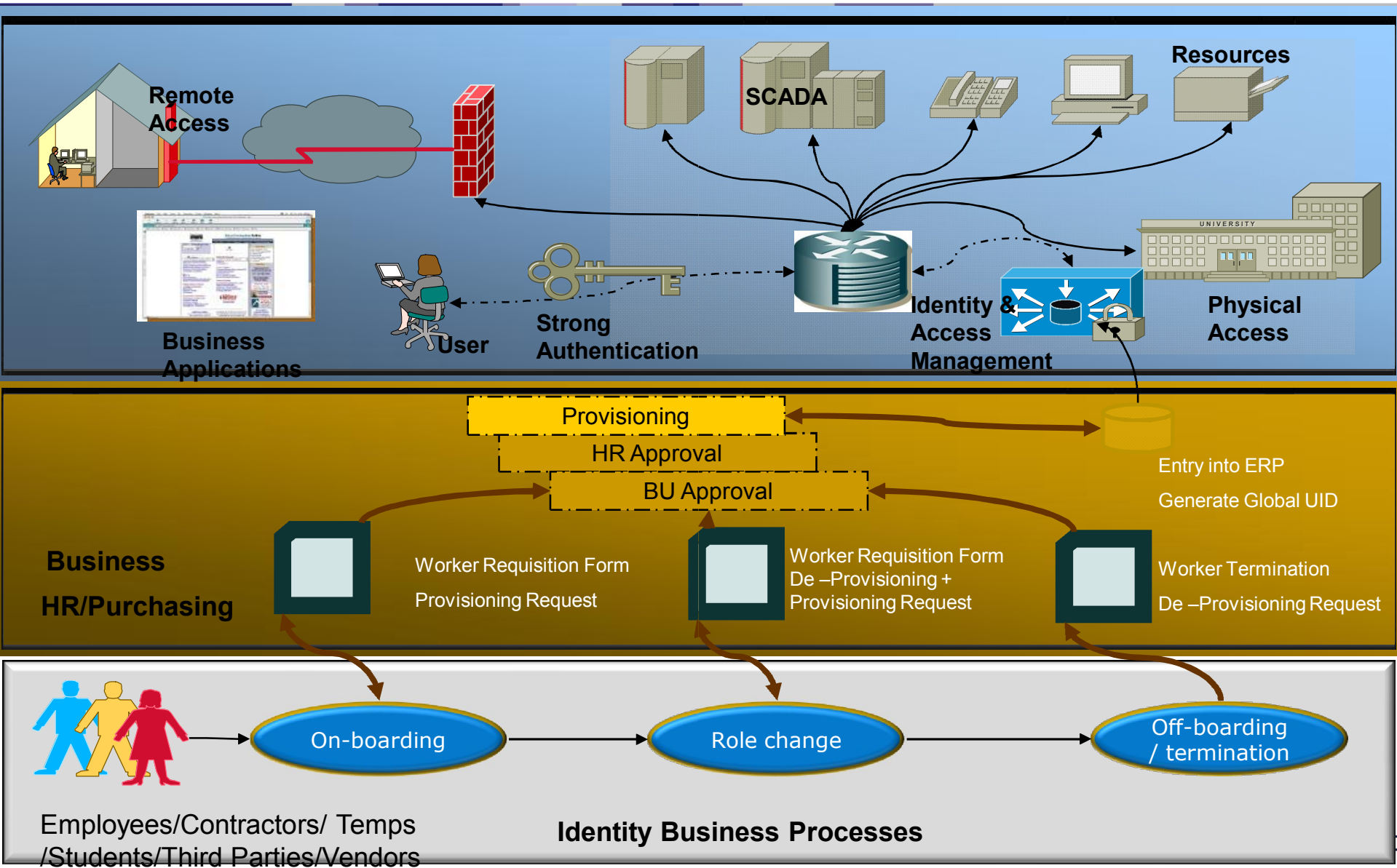
- Cyber security policy and procedures
  - Security policy
  - Standard operating procedures (OPSEC)
  - Guidelines
- Cyber security Planning
  - Strategic planning
  - Tactical planning
- Architecture and technology
  - Network segmentation
  - Tightly controlled communication
  - Identity and access management
  - Threat management
  - Vulnerability management
- Services
  - Certification and Accreditation
- Risk and Security Measurements
  - Security KPI and KRI
  - Real time Security Dashboard



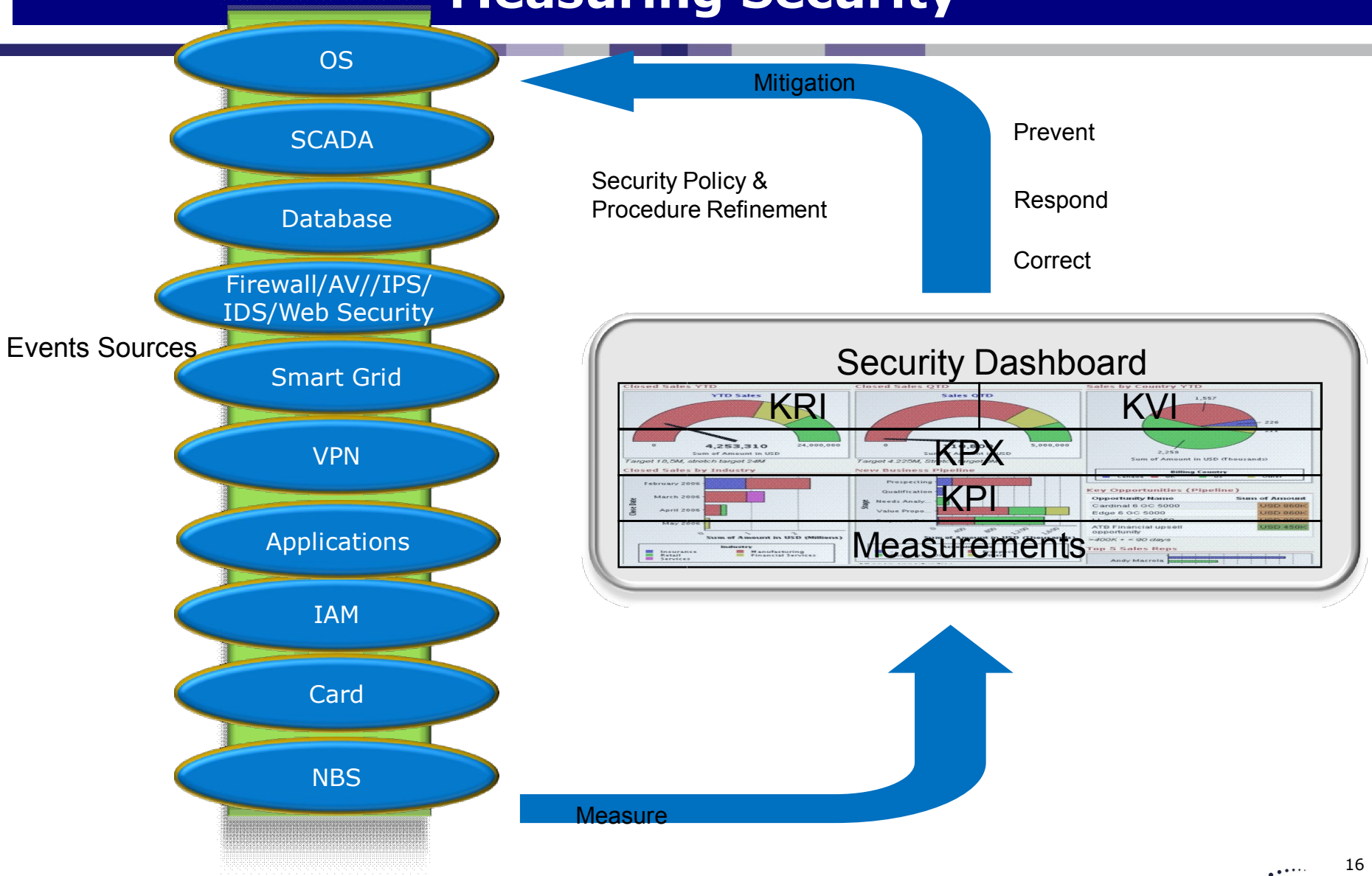
Smart Grid Security Strategy

- Enterprise Defence-in-Depth Strategy
- Security Assessments
- Asset Management
- Network & Application security
- Education and Awareness Program

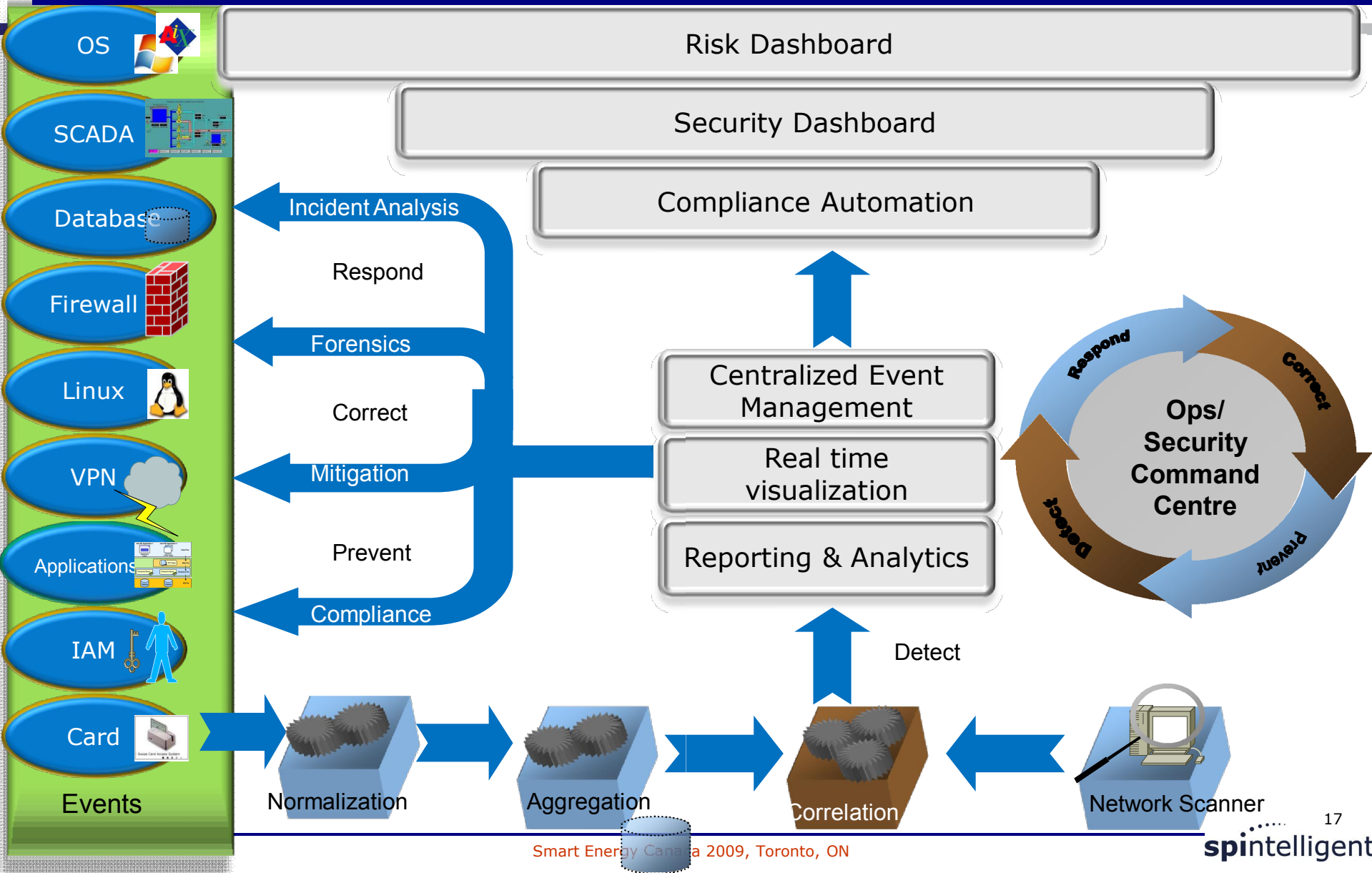
Identity and Access Management



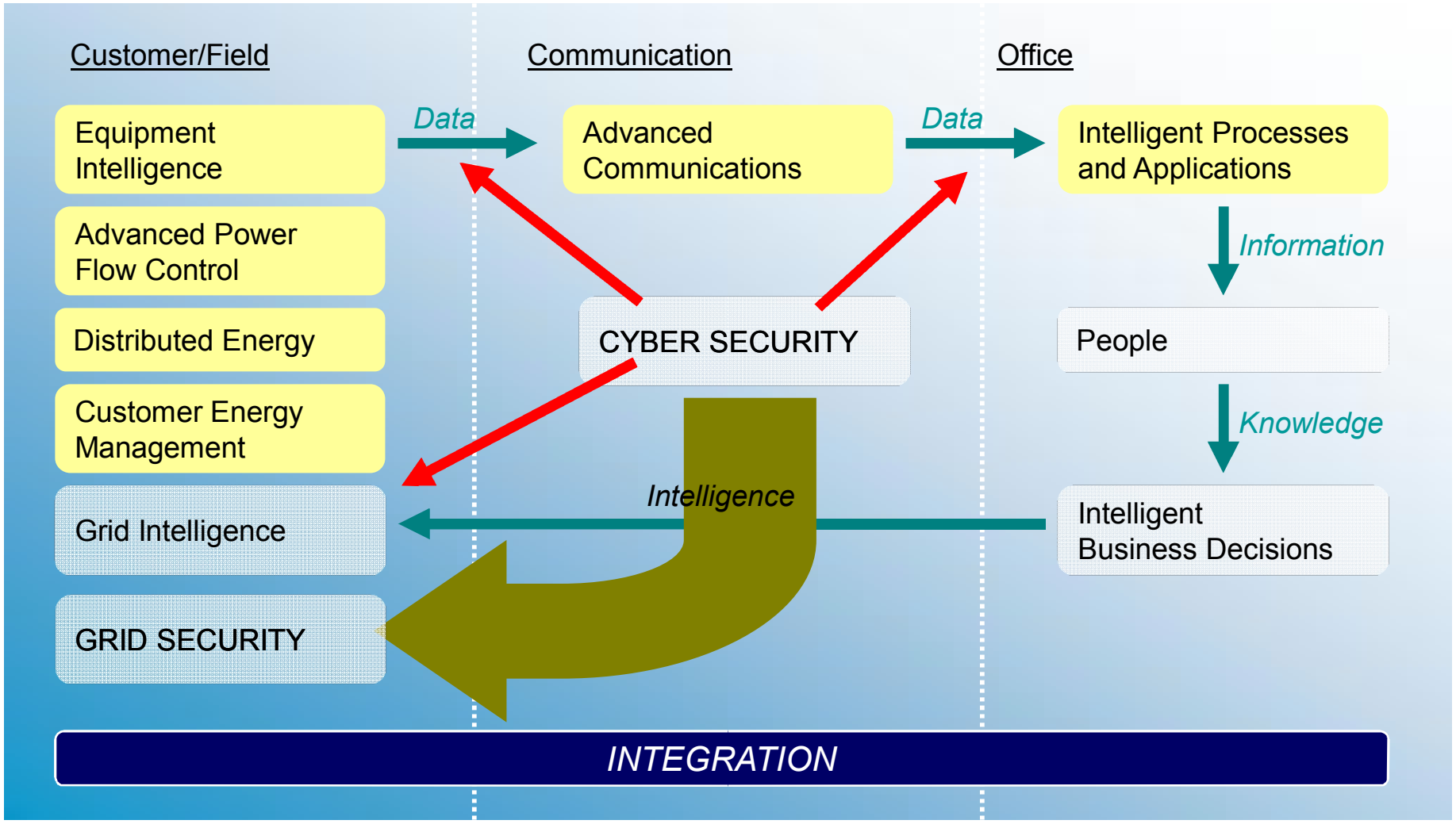
Measuring Security



Measuring Security : Components



Building Security In by 'Defence in Depth'



Expected Gaps and 'Solution' Paths

SECURITY GAPS	POSSIBLE SOLUTION PATHS
Poor protection of critical data	Local encryption; access controls; access management
Inadequate reliability of collection mechanism	Communication authentication and access control
Inadequate security of transmission data	Message digests, point-of-origin validation, intrusion detection, proprietary encryption
Poor redundancy of Storage Protection	Secure network topology
Insufficient device security	Monitors, tamper-proof devices, integrity checking, self-healing networks
Non-scalable Security Solutions	Standards, regulatory efforts, vendor groups
Insufficient security for Customer Presentation	Lifecycle integrity, secure web access, server protection, firewalls, IDS
Insufficient security for Convergence with SCADA and Corporate	Adaptive protection, zones/conduits, multi-tier security, deep-packet inspection

Commercial solutions can be leveraged to support budget and time constraints – but assessments provide tactical understanding!

Q & A

Contact:-

Kshamit Dixit
Toronto Hydro

kdixit@torontohydro.com
416-42-3343