



Smart Grid: Green IT 2.0

A View from Symantec

Symantec Corporation

Jose Iglesias, Vice President

Agenda

1 Introduction

2 Transforming Industry

3 Symantec Vision and Capabilities

4 Questions & Answers

Green IT: Responding to new IT priorities

Green IT 1.0: "Green for IT"

Green IT 2.0: "IT for Green"



Data center and facilities

- IT systems management
- Server and storage virtualization
- Building automation



Distributed IT

- PC power management
- Thin client systems
- Managed print services



Business process and strategy

- Carbon management
- Teleworking
- Supply chain optimization



Public policy and infrastructure

- Smart grid
- Green cities
- Climate change policies

Source: March 5, 2009, "Mapping IT's Green Opportunities" Forrester report

Smart Grid Market Size and Business Drivers

Smart Grid market in North America expected to reach \$18B/year by 2013, \$12B / year for software and IT Services.

(IDC)

- Top 15 AMI deployments in North America: 41.1 million smart meters by 2015
(GTM Research)
- Enel SpA (Italy): installed 30 million smart meters
(GTM Research)



IT spending growth for U.S. utilities 11% in 2010 compared to IT spending growth rate of 2.6% across all industries.

(IDC)

Smart Grid addressable market will grow from \$20 billion in revenue in 2010 to \$100 billion by 2030

(Morgan Stanley)

- DOE top priority: \$3.9B in US ARRA stimulus w/ \$3.3B matching funds
- Global smart meters installed 2008: 46 million; 2015: 250+ million
(Pike Research)

Global smart grid cyber security market to grow to \$4.1 billion in 2013 at a compound annual growth rate of 35%

(Pike Research)

Cisco estimates that the Smart Grid market will grow to \$20B per year within the next 5 years

(San Jose Mercury News 5/18/2009)



The Transformation of the Electrical Grid Will Have a Major Business Impact

Smart Grid – In the Headlines ...



AP Exclusive: `Smart' meters have security holes

Mar 26, 2010

`Smart' meters plagued with serious security holes that threaten power grid

SAN FRANCISCO (AP) -- Computer-security researchers say new "smart" meters that are designed to help deliver electricity more efficiently also **have flaws that could let hackers tamper with the power grid in previously impossible ways.**



MONDAY, MARCH 29, 2010

Internet-Brewed Coffee? Maybe Not, but Much, Much More

At the CTIA Wireless trade show in Las Vegas last week,... the astonishing forecast made at the show by Cisco Systems' (CSCO) chief technology officer, Padmasree Warrior. She asserted that sometime in **2013, there will about one trillion -- trillion! -- devices connected to the Internet.**



3/21/2010

Academic Paper in China Sets Off Alarms in U.S.

Larry M. Wortzel, a military strategist and China specialist, told the House Foreign Affairs Committee on March 10 that it should be concerned because "Chinese researchers at the Institute of Systems Engineering of Dalian University of Technology published a paper on how to **attack a small U.S. power grid sub-network in a way that would cause a cascading failure of the entire U.S.**"



Mar. 17, 2010

FCC Release National Broadband Plan, Privacy Strategy Unclear:

The [Federal Communications Commission](#) (FCC) released its [National Broadband Plan](#) today. The FCC notes that "**many users are increasingly concerned about their lack of control over sensitive personal data**" and warns that "Innovation will suffer if a lack of trust exists between users and entities with which they interact over the internet." The FCC makes several recommendations, but there is **no clear plan to address growing concerns about ... smart grids....** Last year, EPIC [urged](#) the FCC to develop a comprehensive strategy for online privacy as part of the national broadband strategy.



November 19, 2009

As Smart Grid Expands, So Does Vulnerability to Cyber Attacks

...head of the nation's electric grid operations monitor, Rick Sergel is warning the power industry that if it doesn't move faster and harder to protect itself against cyber threats, Congress and federal regulators will increasingly impose their own rules.

The danger goes beyond the disabling of transformers and control systems to include the **"kidnapping" of key devices by attackers who would try to send spurious signals to shut down customers' smart meters or take power plants offline**, says Joseph McClelland, director of the Office of Electric Reliability at the Federal Energy Regulatory Commission.



3/20/2009

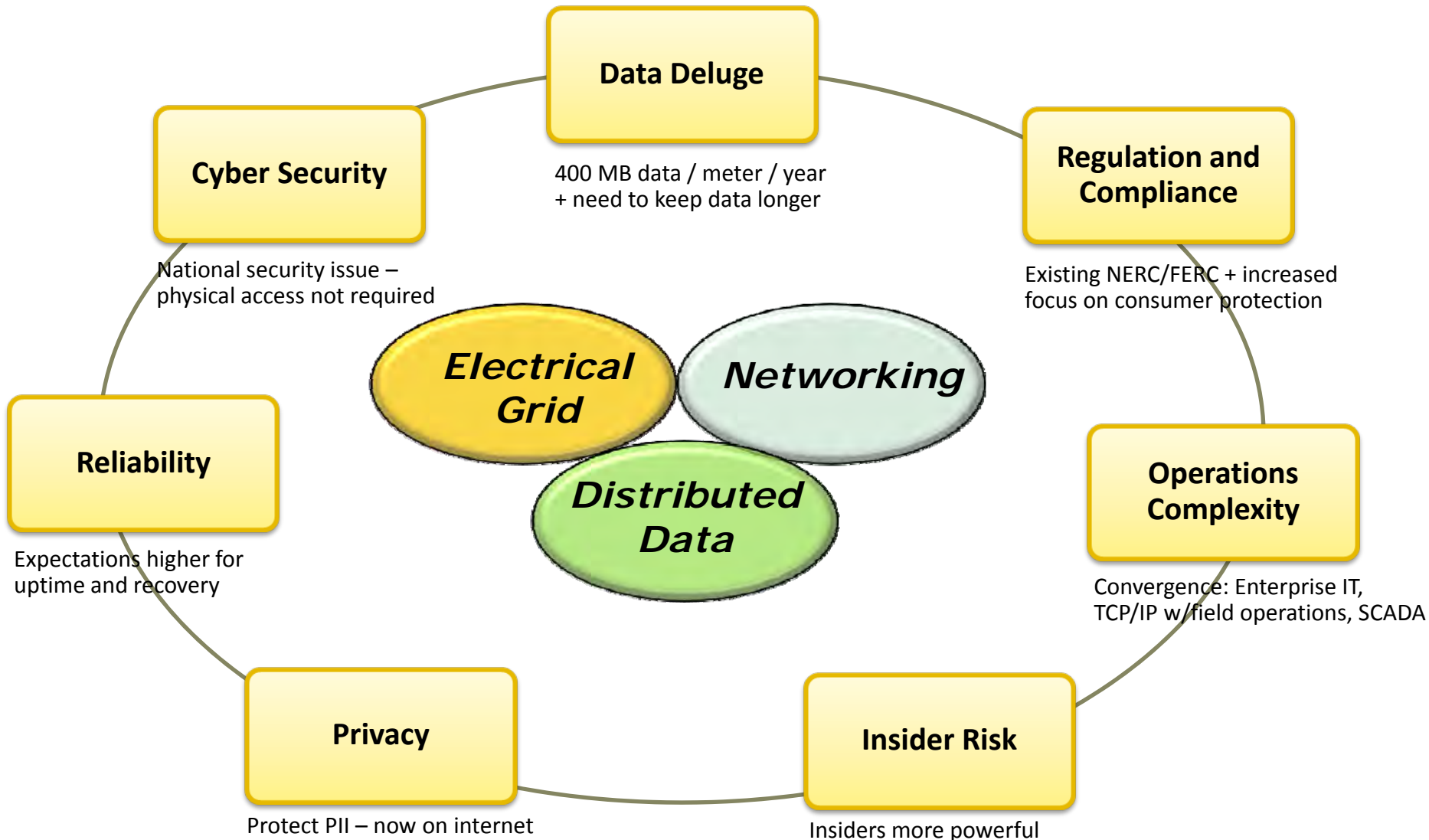
'Smart Grid' may be vulnerable to hackers

But cybersecurity experts said some types of meters can be hacked, as can other points in the Smart Grid's communications systems. IOActive, a professional security services firm, determined that **an attacker with \$500 of equipment and materials and a background in electronics and software engineering could "take command and control of the [advanced meter infrastructure] allowing for the en masse manipulation of service to homes and businesses."**







Smart Grid Concerns Growing ... a matter of national importance

Utility Industry is Transforming

Management of Data / Event / Compliance / Security



Critical Points

IT Back-End	GENERATION	TRANSMISSION	SUBSTATION	DISTRIBUTION	CUSTOMER
					
Customer Billing ERP Some Operations	Generation & Network Operation Center	Transmission - Distribution Sub- station Transmission	Substation	Distribution & Transformers	Consumer , Commercial & Co-generation

Electrical Grid

- Matter of National security
- Energy Independence
- Timely Response for updates
- Outage (FLIR), voltage, phase, and frequency data, along with detailed status and diagnostic information
- Grid health understood across all sectors

Networking

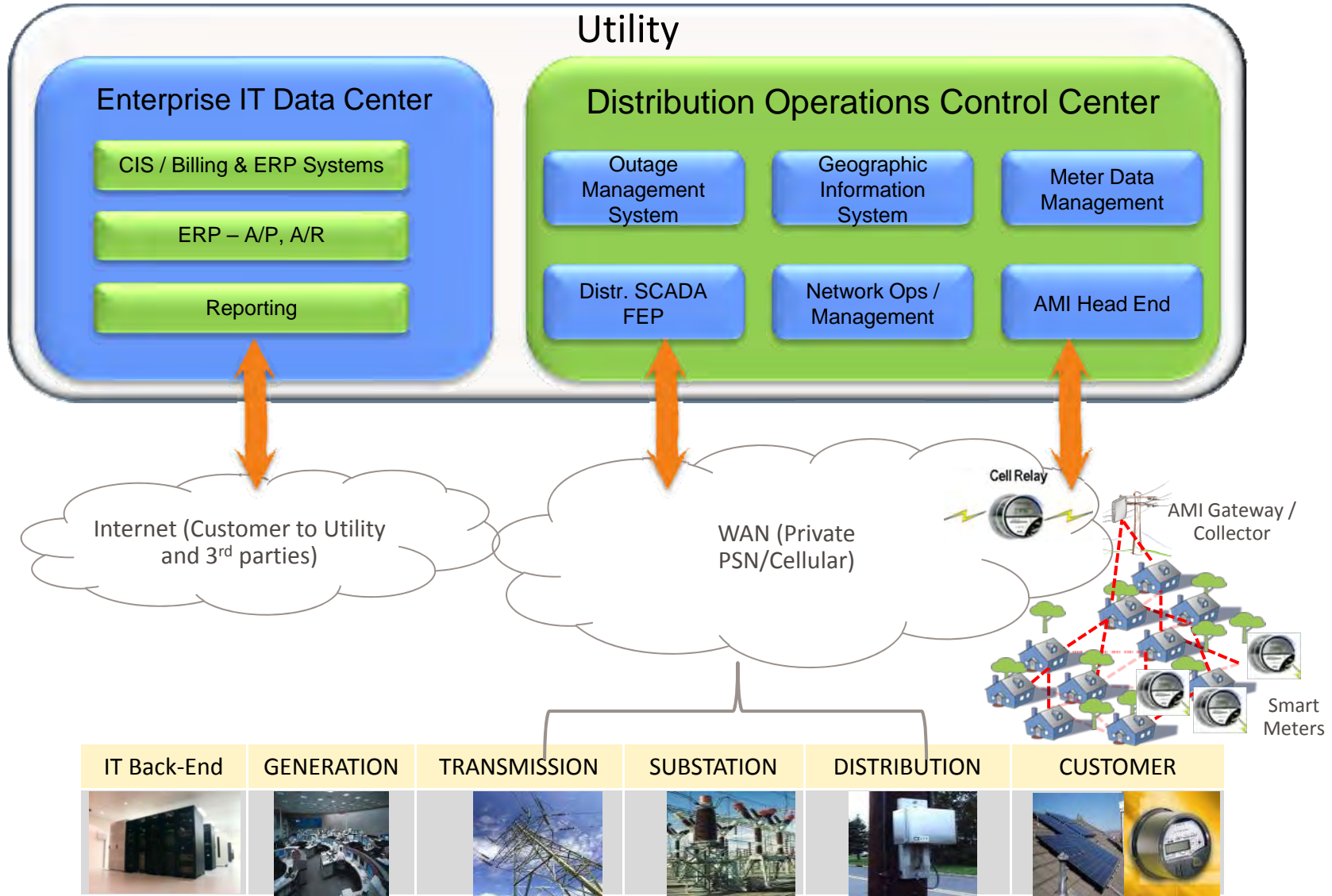
- Integration of networked sensors
- Identify Outages (FLIR)
- Triangulate the fault source, ability to correlate distributed data
- Ensure timely updates to device / system software
- AMI deployments
- Network Generation ... AMI

Distributed Data

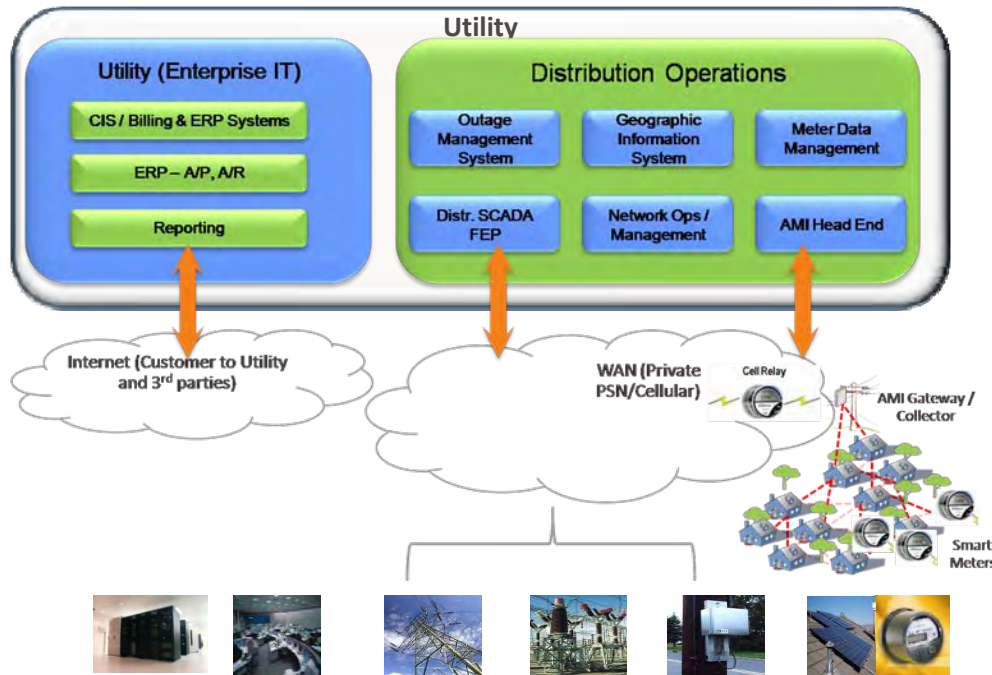
- Data Growth is staggering
- Data sharing between competitive utilities on load and demand
- Retention and recovery requirements
- Large amounts of historical data for trend analysis
- Long term and cost-effective storage will continue to be in the forefront.

Information about the Grid is Critical

More Networking, More Opportunities, More Challenges



Information Must Be Tracked, Managed and Protected



Exploding Data Volume

- Need for efficient Storage management

Data Protection

- Efficient data backup
- Archiving access

Privacy

- Personally Identifiable Information (PII) must remain protected

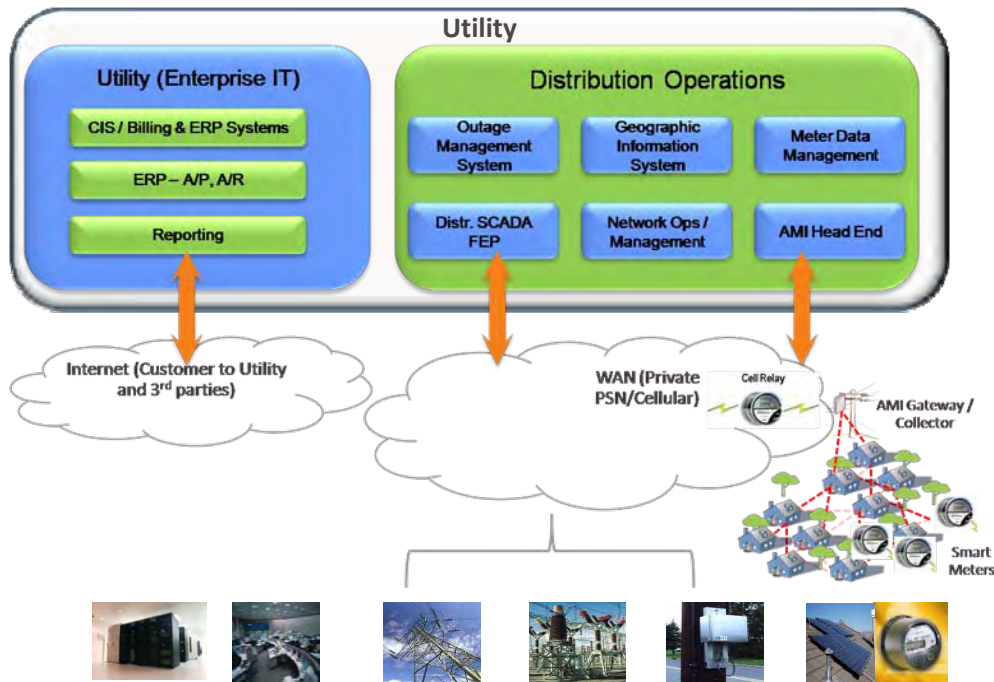
Regulatory

- Tracking meter data with billing information – verification
- Accuracy, Auditing, Retention

Archive, Search, Catalog

- Need access and control of internal information

Comprehensive, Layered Approach to Security Required



Internal Threats

- Insider threats more powerful (classification & authentication of information)

Field security

- Wireless/ Cellular security
- Key management
- Authentication

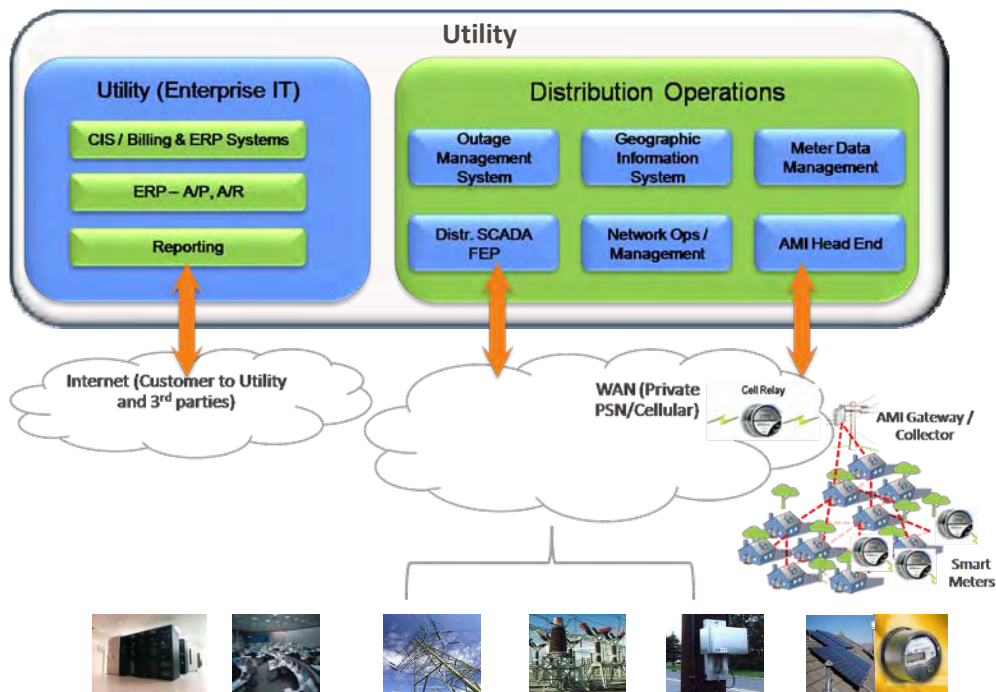
HAN security

- Weak security for home PC authorized to access meter info

Network Security

- Perimeter protection
- Threat Containment & Isolation
- Intrusion Protection
- Event correlation

Management is an Ongoing Problem Dependent on Standards and the Convergence of Diverse Technologies & Processes



Outage Management

- Correlation of multiple data sources for outage detection, scoping, recovery (FLIR) w/security databases

Management Complexity

- Convergence of Enterprise COTS, and Legacy technologies
- Integration of EMS, SCADA, AMI, MDM, GIS, DMS, asset management

Endpoint Management

- Endpoints updated w/latest security fixes, patches
- Asset, version control information

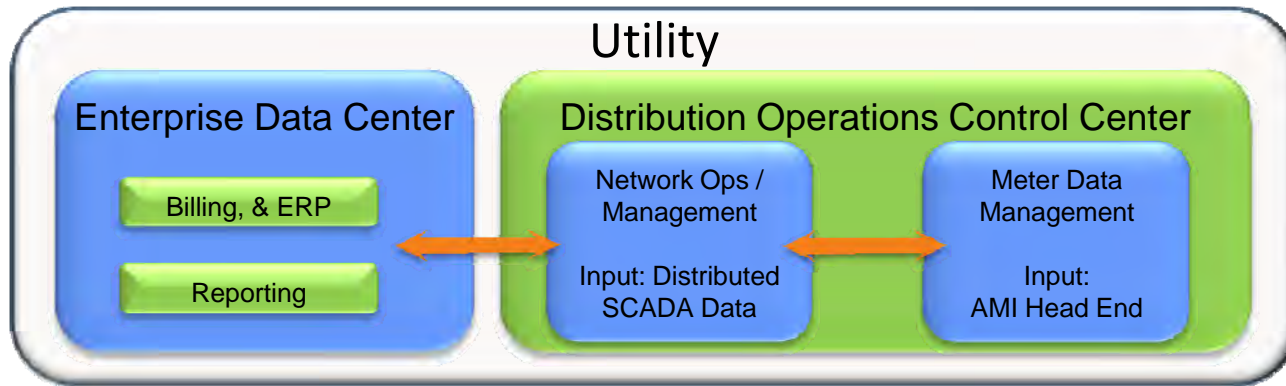
Grid Management

- Detecting Outages
- Remote monitoring and control
- Load flow analysis and control

New Standards

- Standards will take time (IEC 61850, 61968, DNP3, NISTIR,...)

Smart Grid Use Cases – Before and After



NERC CIP Compliance

Before

1. Large utility-wide team manual review of NERC Critical Infrastructure Protection (CIP) requirements – not comprehensive across control systems & domains
2. Security experts not available in Operations Control Center; IT not available 24x7

After

1. NERC CIP compliance - small team + security **compliance tools** to **automate** audit, monitoring & reporting; **import data** from security infrastructure
2. **Comprehensive** set of security tools & systems for IT, SCADA, EMS, DCS systems (ICCP, ModBus, IP protocols).
3. IT Data Center, Control Center and field networks – **automated, integrated & continuous** monitoring against security policy (vulnerabilities, controls, access, change management, firewalls, etc)

Outage / Recovery (FLIR)

Before

1. Utility detects outage when calls come into Call Center around 5PM (after customers return home from work)
2. Utility attempts to triangulate outage scope from call center information
3. Utility must send out staff to determine root cause

After

1. Utility **detects outage** utilizing MDM data, SCADA data event correlation in near real-time
2. **Outage scope** from correlation w/ location data
3. **Root cause** ascertained by correlation with weather, fire, security data
4. Automated **workflow** initiated (w/human intervention)
5. Decision: send after hours field technicians, or re-route power & **send field personnel at optimal time**

A Very Challenging Environment Moving Forward

Data Deluge & Complexity

Data Growth & Complexity

Data storage, data availability & storage management needs due to MDM, SCADA, other DBs growing w/more analytics, reporting & trending needed; Archiving & auditing - up to 7 years;

Outage Management

Identify anomalies, detect outages; Fault Location, Isolation & Service Restoration (FLISR) w/root cause analysis, remediation & recovery

Availability

Threats

Insider threats; internet based attacks, malware; authentication and key management concerns; local vulnerabilities & system-wide threats; energy theft

Security & Insider Risk

Endpoint Management

Proprietary systems (SCADA, networks) mixing with COTS IP-based technology; convergence of Enterprise IT and legacy field operations practices; managing complexity for millions of endpoints

Management

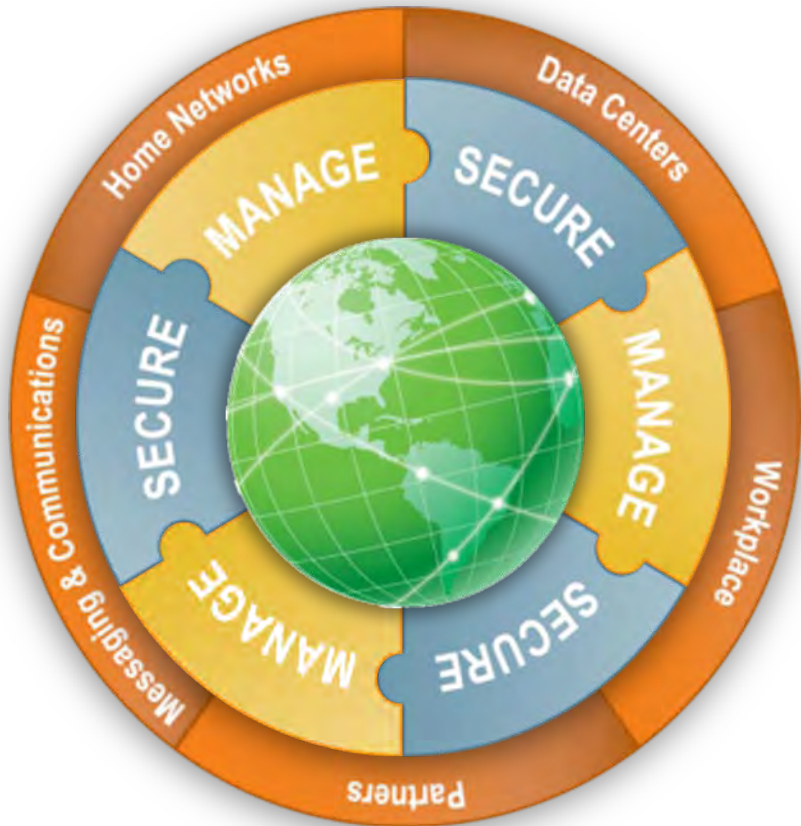
Compliance and Privacy Protection

*NERC / FERC regulatory requirements
Customer data privacy (PII) protection essential
Billing verification*

Compliance & Privacy

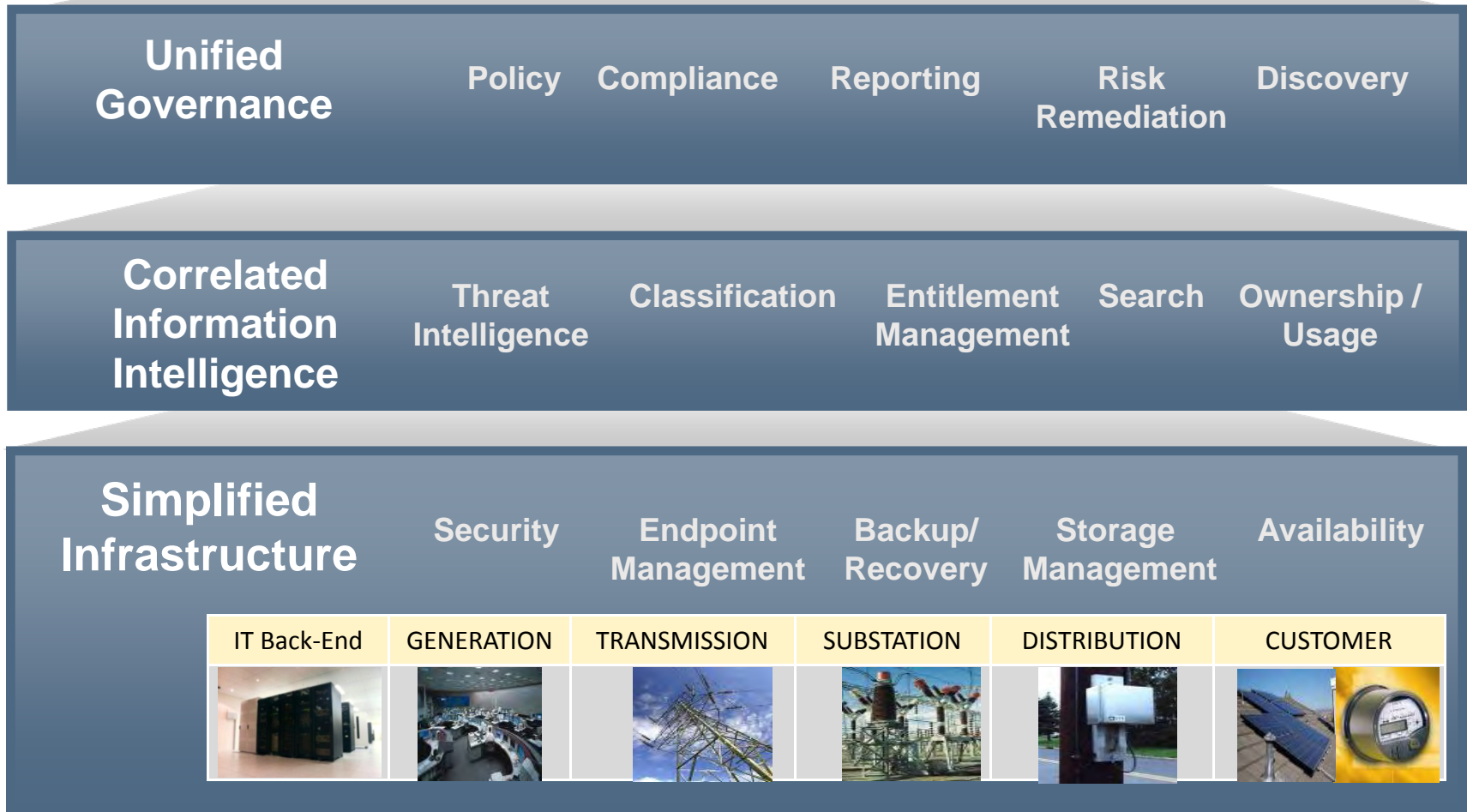
Symantec Vision and Capabilities

Symantec Strategy: Secure & Manage Your Information - from Control Center to Customer









- Focused on **information**, not on systems or proprietary stacks
- *Unified Information Governance*
- *Correlated Information Intelligence*
- *Simplified Information Infrastructure*

Information-Centric Security and Management



Symantec Capabilities







IT Back-End	GENERATION	TRANSMISSION	SUBSTATION	DISTRIBUTION	CUSTOMER
					
Customer Billing ERP Some Operations	Generation & Network Operation Center	Transmission - Distribution Sub- station Transmission (Step-down Transformer)	Substation	Distribution & Transformers	Consumer, Commercial & Co-generation

Today

- Compliance
- Correlation & Reporting
- Data Storage & Availability
- Data Protection & Archiving
- Malware Protection/Discovery
- Zero Day Protection
- Behavioral based design
- Data Loss Prevention
- Outage & Disaster Recovery
- Advanced Workflow and Automated Remediation Technology
- Cost Effective Solutions

Security and Management for the Smart Grid

Symantec Capabilities

IT Back-End	GENERATION	TRANSMISSION	SUBSTATION	DISTRIBUTION	CUSTOMER
					
Customer Billing ERP Some Operations	Generation & Network Operation Center	Transmission - Distribution Sub- station Transmission (Step-down Transformer)	Substation	Distribution & Transformers	Consumer , Commercial & Co-generation

Today







- Compliance
- Correlation & Reporting
- Data Storage & Availability
- Data Protection & Archiving
- Malware Protection/Discovery
- Zero Day Protection
- Behavioral based design
- Data Loss Prevention
- Outage & Disaster Recovery
- Advanced Workflow and Automated Remediation Technology
- Cost Effective Solutions

Tomorrow

- Extend the Defense Perimeter
- Embedded Device Security: leverage mobile security of embedded, non-PC O/S, ARM, similar to Smart Meters)
- Event and Outage Correlation
- Grid Security Breach Detection
- Maintain Device Integrity (Up to date updates and provisioning of firmware updates and patches, signatures)
- Proactive IDS/IPS Server Security w/ Network Firewalls w/ Zero Day Protection & Behavioral based design

Security and Management for the Smart Grid

Symantec Capabilities

IT Back-End	GENERATION	TRANSMISSION	SUBSTATION	DISTRIBUTION	CUSTOMER
					
Customer Billing ERP Some Operations	Generation & Network Operation Center	Transmission - Distribution Sub- station Transmission (Step-down Transformer)	Substation	Distribution & Transformers	Consumer, Commercial & Co-generation

Today

- Compliance
- Correlation & Reporting
- Data Storage & Availability
- Data Protection & Archiving
- Malware Protection/Discovery
- Zero Day Protection
- Behavioral based design
- Data Loss Prevention
- Outage & Disaster Recovery
- Advanced Workflow and Automated Remediation Technology
- Cost Effective Solutions

Tomorrow

- Extend the Defense Perimeter
- Embedded Device Security: leverage mobile security of embedded, non-PC O/S, ARM, similar to Smart Meters)
- Event and Outage Correlation
- Grid Security Breach Detection
- Maintain Device Integrity (Up to date updates and provisioning of firmware updates and patches, signatures)
- Proactive IDS/IPS Server Security w/ Network Firewalls w/ Zero Day Protection & Behavioral based design

Standards and Partners

- Standards Engagement – Member of Electrical Power Research Institute (EPRI), NIST Smart Grid Interoperability Panel (SGIP,) OpenSG (Open Smart Grid Users Group), SNIA GSI, and the Green Grid (TGG)
- Reaching out to equipment providers
- Cellular and Wireless Security partners (AT&T, Sprint, Verizon)
- Integrators Partners (Accenture, ...)

Security and Management for the Smart Grid

Symantec Technology Solutions to Smart Grid Challenges

Data Deluge & Complexity

Data Growth & Complexity

Storage Foundation-HA, Command Central Storage, Netbackup, Backup Exec, Enterprise Vault, Control Compliance Suite, Data Loss Prevention, Cloud based Data Protection

Availability

Outage Management

Symantec Security Information Manager, Symantec Workflow Engine, CMDB; SF/HA and Clustering for failover and disaster recovery

Threats

Infrastructure Protection: SEP, Critical System Protection; Insider Threat: Data Loss Prevention; Field security: NAC, SEP for Embedded, MSS Deepsight, Cloud based security & Key Mgmt

Endpoint Management

Endpoint Management Solutions: Server Management Suite, Client Management Suite, Configuration Management Database (CMDB), LiveUpdate

Security & Insider Risk

Management

Compliance and Privacy Protection

Control Compliance Suite, Data Loss Prevention

Compliance & Privacy



Thank you!

Jose Iglesias

Jose_Iglesias@symantec.com

650.527.2187

Copyright © 2010 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.