



## Cyber Security in the Electricity Industry

Gib Sorebo, Assistant Vice President/Chief Cyber Security Technologist

National Association of Regulatory Utilities Commissioners (NARUC) Conference  
November 2009



# Why Should a Commissioner Care About Cyber Security?



“The Commerce Commission ... shall examine those public utilities and keep informed as to their general condition, their franchises, capitalization, rates and other charges, and the manner in which their plants, equipment and other property ... are managed, ... not only with respect to the adequacy, **security** and accommodation afforded by their service but also with respect to their compliance with this Act and any other law...” (220 ILCS 5/4-101)



“The Commission shall require all public utilities to establish a security policy that includes on-site safeguards to restrict physical or electronic access to critical infrastructure and computerized control and data systems. The Commission shall maintain a record ...:

- (1) that the entity has a security policy in place;
- (2) that the entity has conducted at least one practice exercise based on the security policy ... and
- (3) ... that the entity follows ... the most current security standards set forth by the North American Electric Reliability Council.” (220 ILCS 5/4-101)

# The Segmented Nature of Cyber Security



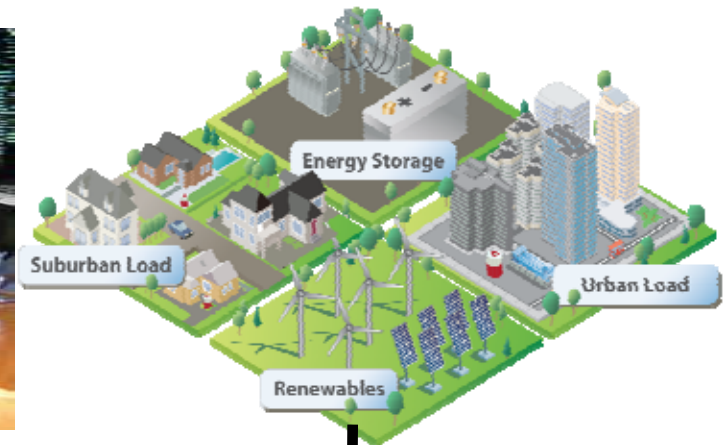
## Traditional IT



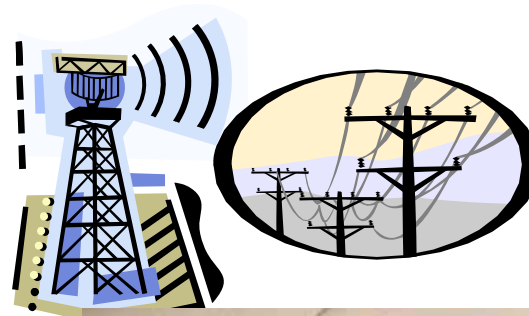
## Traditional OT



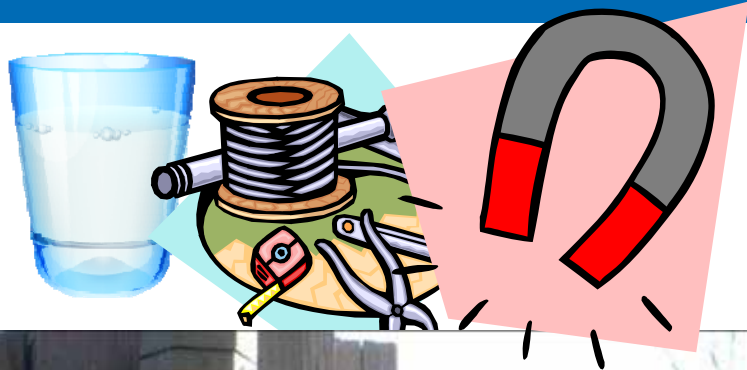
## “Smart Grid”



# So What's Changing?



# And the Threats?



## Threats Are Real



Brazil electricity  
outages blamed on  
cyber attacks  
**60 Minutes, Nov. 8, 2009**

“Electricity Grid in  
U.S. Penetrated By  
Spies”  
**Wall Street Journal,  
April 8, 2009**

“Copper Thieves Threaten U.S. Infrastructure, FBI says”  
Wired Magazine, December 3, 2008

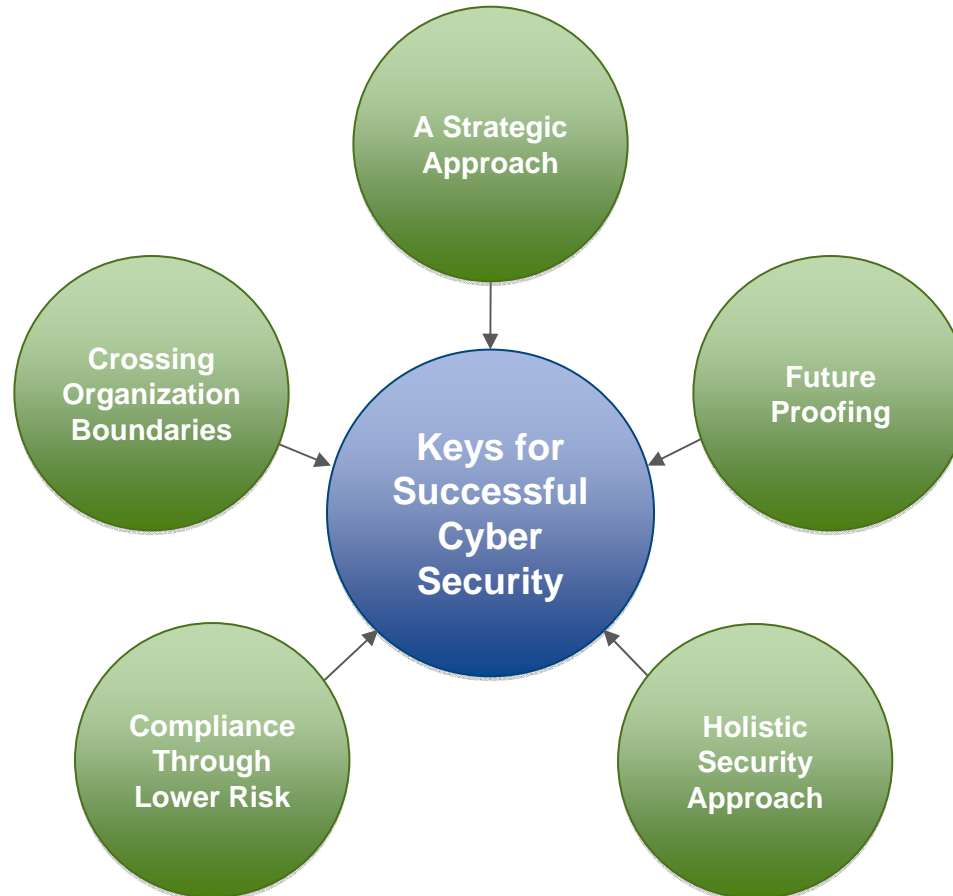
## And so Are the Harms...



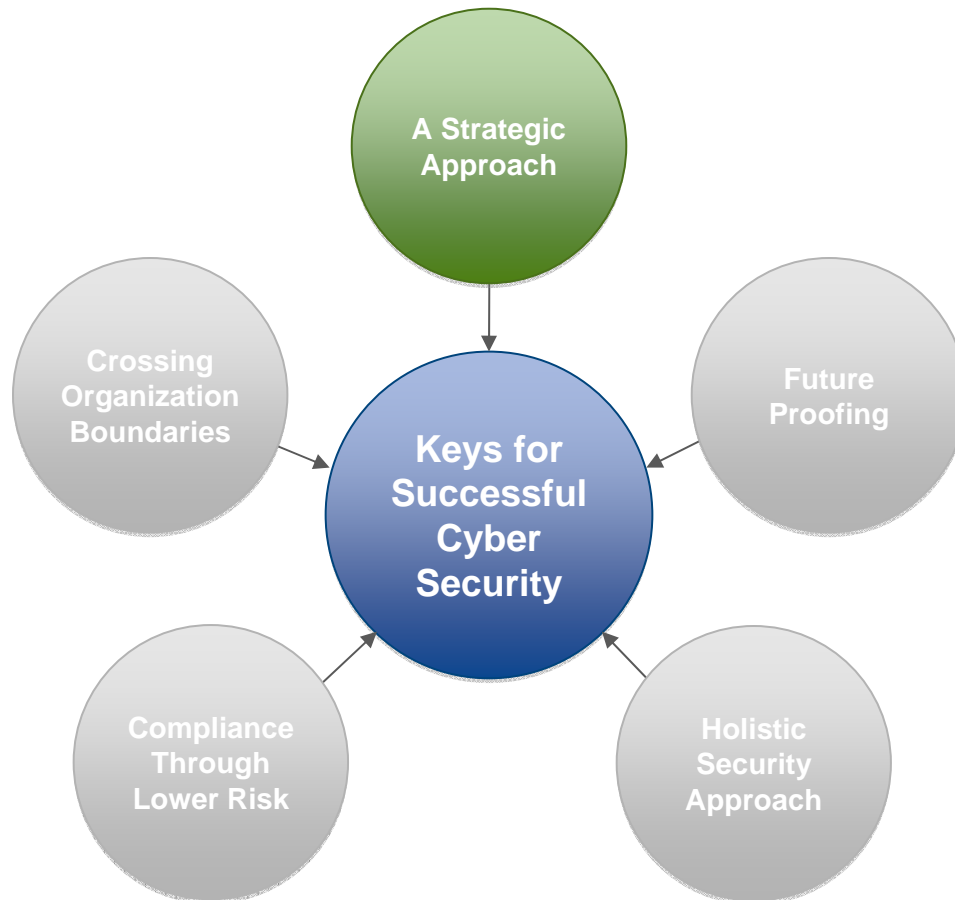
Photos from U.S. Geological Survey, USGS/Rolla, Mo. Used with permission.

- **1998:** Telephone switch hack closes an airport
- **2000:** Gazprom central control is hacked
- **2000:** Australian hacker causes environmental harm by releasing sewage
- **2001:** Hackers protesting U.S./China conflict enter U.S. electric power systems
- **2003:** Power outages in northeastern United States occur
- **2003:** Worm shuts systems down at Davis-Besse nuclear plant
- **2006:** Zotob virus shuts down Holden car manufacturing plant
- **2007:** Aurora demonstration shows damage a remote hacker can cause physical harm to a generator

# Keys for Successful Cyber Security



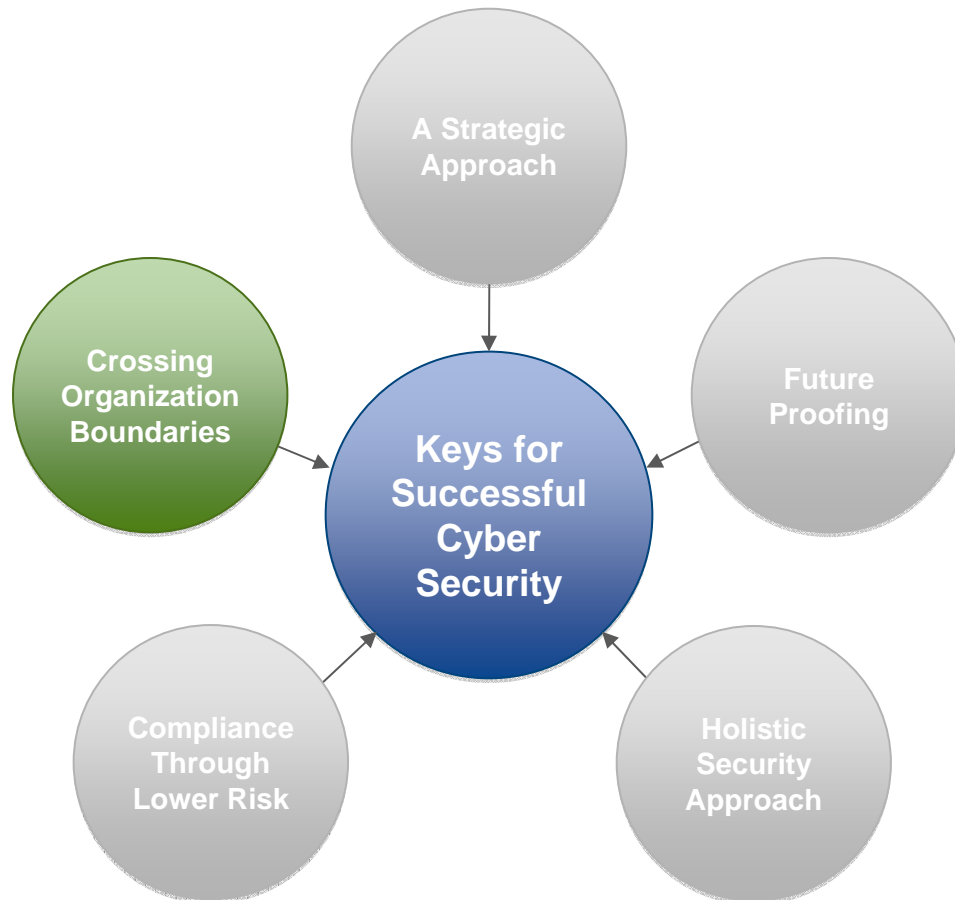
# A Strategic Approach



“Technology without strategy is chaos.”

- Boxes, services, audits, testing, software, widgets
- What does it all mean?
- Will any of it work together?
- You don’t buy software without some kind of enterprise strategy
- Don’t try to secure critical infrastructure investments without one!

# Crossing Organizational Boundaries



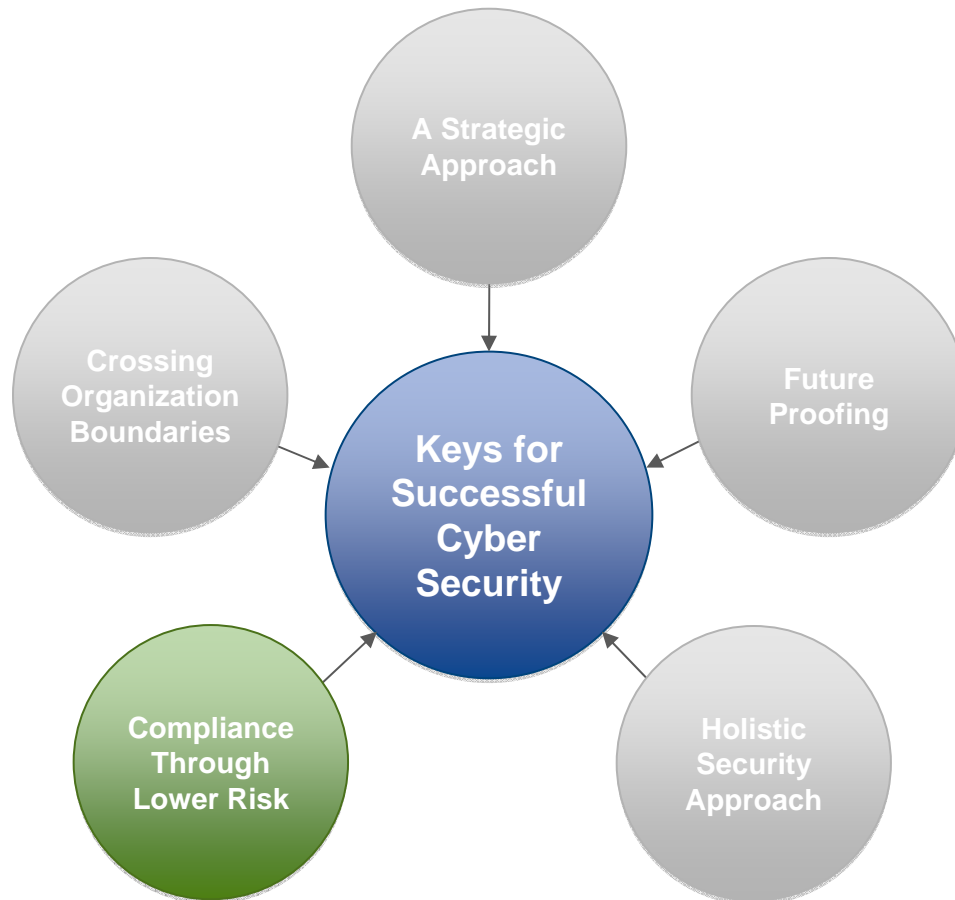
A technological and process transformation of the business cannot happen with static and stove-piped organizations.

- Enterprise IT has a lot to offer in managing these types of challenges
- Not a perfect fit, but a start
- How can it be adapted to an adjusted mission?
- Reinventing the wheel elsewhere can be expensive and challenging

IT = Information Technology



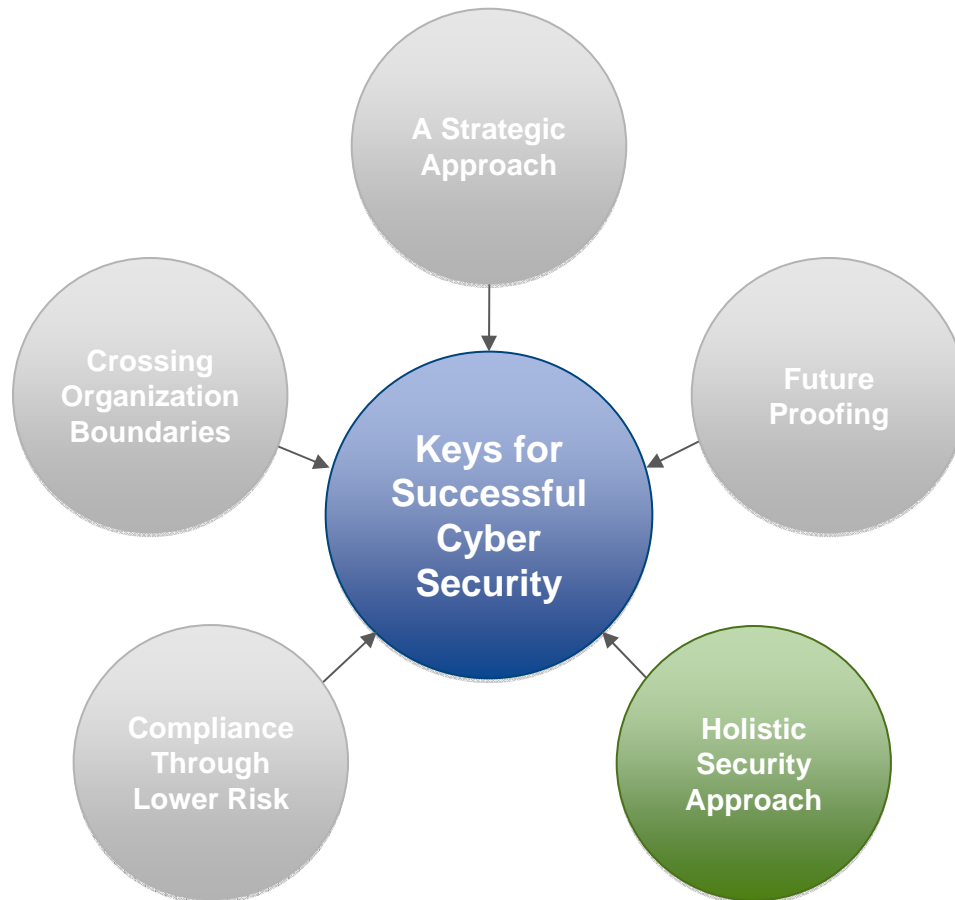
# Compliance Through Lower Risk



Compliance is not security, nor is it risk management

- Don't wait for mandates to define your minimum obligations. It likely will not address your real security needs.
- Considered and appropriate risk management strategies and security solutions will line up with mandates. The reverse is not necessarily true.

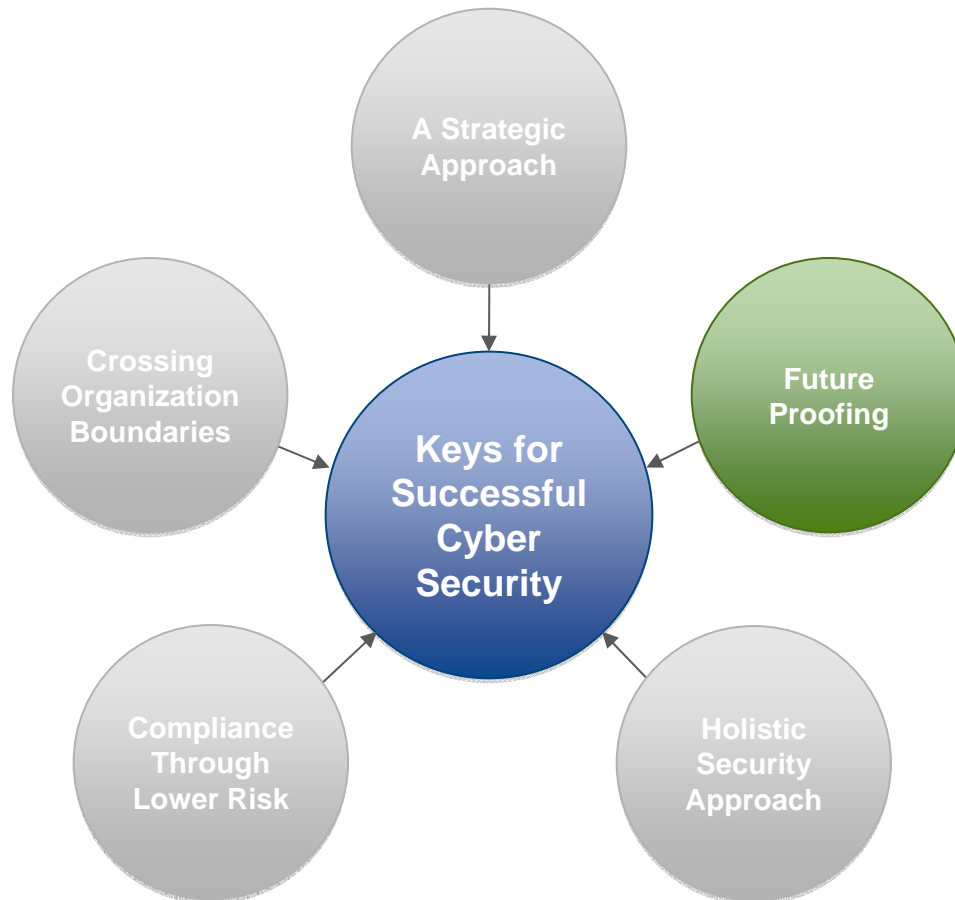
# Holistic Security Approach



Focus beyond the asset  
“capabilities” discussion

- Understanding capabilities is part of developing and implementing a security response to risk
- People and processes are what will help to ensure actual security every day afterwards
- Don't follow the marketplace trap of assuming “the box/vendor does that.” The box does not manage anything; it just does what it is told.

# Future Proofing



Defending a 20-year field-investment will necessarily flex the latter portions of the security life cycle, so consider it up front

- Protect against what you know are issues
- Monitor and measure proactively to manage complexity and internal risks
- Respond to new threats with dedicated resources
- If you are going to do it yourself, know what you are getting yourself into

# Talking Points for Discussion



## For Public Utilities Commissions

- Ask how security is addressed for each component
- Don't accept assurances that all products used were built to be secure
- Ask to see risk assessment documentation
- Ensure security is budgeted for and individuals are assigned responsibility

## For Utilities

- Insist that vendors document independently verify their security controls
- Ensure service providers (for example, telcos, meter data processors) are included in risk assessment and provide sufficient information
- Integrate security between operations and enterprise

# Thank you



## **Gib Sorebo**

SAIC AVP/Chief Cyber Security Technologist

*tel:* 703-676-2605 | *email:* [sorebog@saic.com](mailto:sorebog@saic.com)