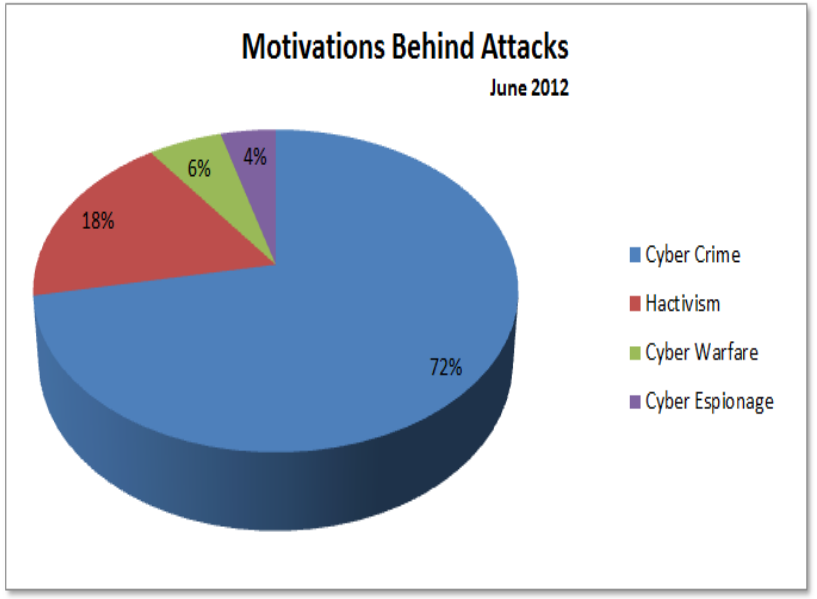
Lessons Learned In Smart Grid Cybersecurity

Chris Blask
Chair
ICS-ISAC
TCIPG Workshop, October 30, 2012

Cyberwar Hits Energy Firms

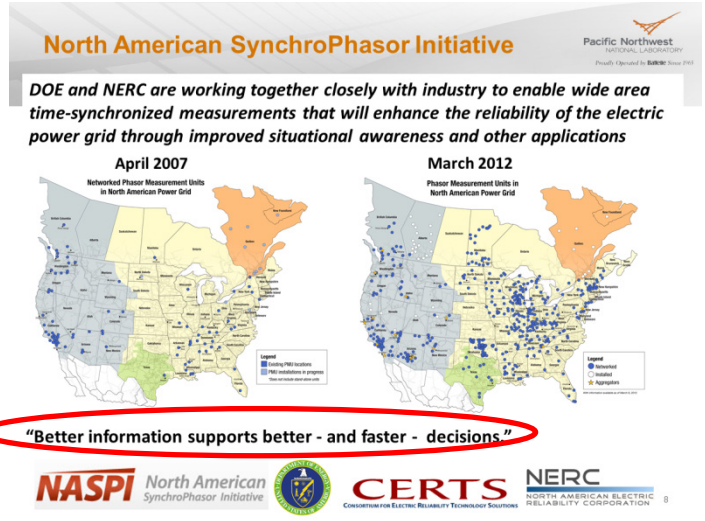
- Escalating from Interruption to Destruction
  - Iranian nuclear program: Stuxnet destroys 1,000+ centrifuges
  - Saudi Aramco: 30,000 systems destroyed; Qatar RasGas similar impact
  - State-sponsored hacking attacks against energy sector rising



* Chart: Paolo Passeri, July 13 2012 http://hackmageddon.com/2012/07/13/june-2012-cyber-attacks-statistics/

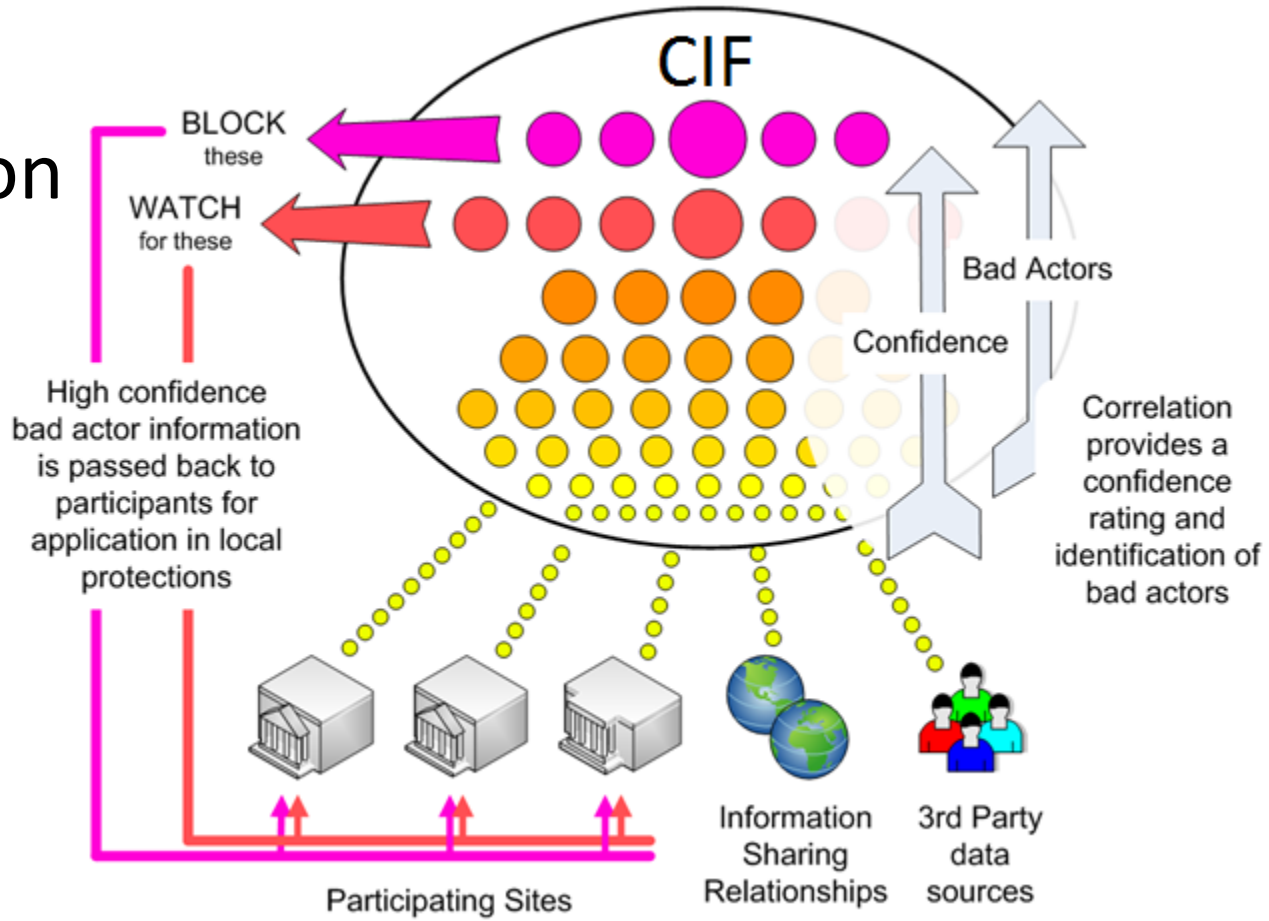
Knowledge is Power

- Knowledge of:
  - What you have
  - What it is doing
  - What is happening around you
  - What the threats are
  - What the risks are
  - What the costs are
  - What others are doing



Knowledge Sharing Works

- REN-ISAC saving universities “100s of $M”
- Five indicators
- Active protection



We Cannot Remediate to Security

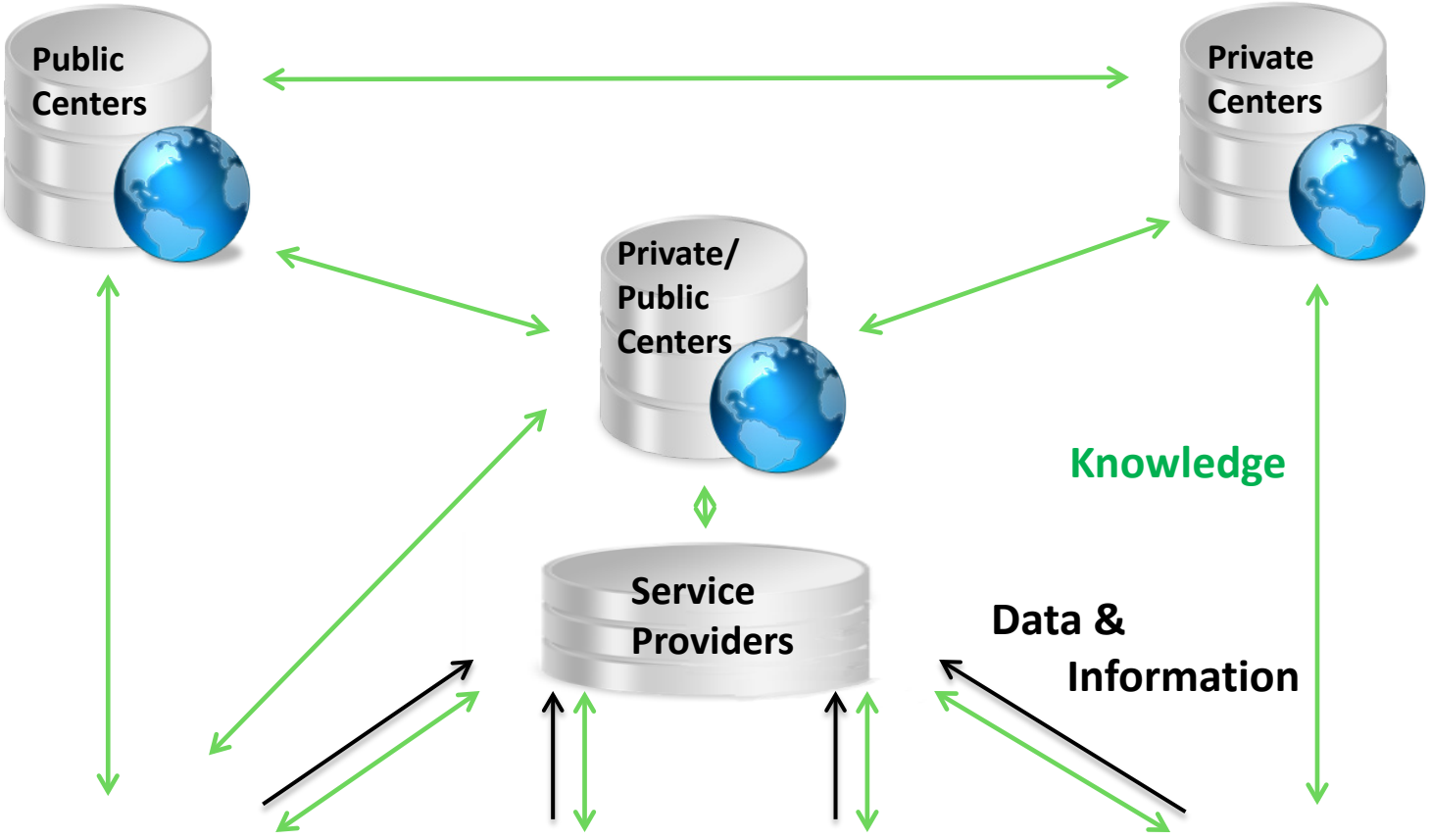
- These are all Good:
  - Vulnerability Assessments
  - Patch Management
  - Vendor Security Improvements
  - NERC CIP

- But do not lead to secure systems

Working Together Works

- Researcher with one computer finds 500,000+ control systems connected to Internet
- Beyond the scope of public sector to address
- Private sector working group forming to work on this and similar datasets

Knowledge Sharing Networks Work







ICS-ISAC

Real Time Knowledge Sharing Works

Integrators

Knowledge Centers

Vendor/ Researcher

ICS-ISAC

MSSPs

Vendor Offices

CERTs

Data, Information and Knowledge

- Data: Items Specific to Devices and Sites
- Information: Data Aggregated to Provide Facilities Operational Visibility and Defense
- Knowledge: Actionable Sharable Intelligence
  - Anonymized to address utility and legislative needs

Nothing Succeeds Like Success

SSEB Cyber Threat Initiative

- One Year Multi-State Cyberwar-Network Pilot
  - Volunteering utilities from 16 Southern States and 2 territories
  - Passive network for visibility, threat analysis, and knowledge sharing across the region
- From Knowledge Sharing to Intelligence
  - Among state and interstate stakeholders
  - Benchmark and pattern-match emerging threats to architect self-learning cyber infrastructures
- Upgrade Real-time Monitoring Cyberwar Network
  - Within two quarters of operations
  - Built-in Cyber-Immune Infrastructure
  - Goal: Energy security and economic stability

Lessons Learned: The Future is Shared

- Knowledge Sharing Key to Active Defense
- Share Skills Between IT and OT
- Private Sector Needs to Share in Leadership
- Action Leads to Solutions

Thank You

Chris Blask
Chair
chris@ics-isac.org