

Realtime Knowledge Sharing For Active Protection

Chris Blask: ICS-ISAC

Gib Sorebo: SAIC

ICSJWG Fall 2012



Challenges to Infrastructure Protection

- A Lot of Work, a Little Protection
 - Pen Tests, Vulnerabilities, Guidelines, ...
- Solution Growth not Mapping to Risks
 - Threat curve outpacing protection
- Impact of Failure to Address Risk Excessive
 - Aug 15 - Saudi Aramco: 25% of global oil
 - Aug 27 - RasGas Qatar: 28% of global natural gas



Active Protection Model

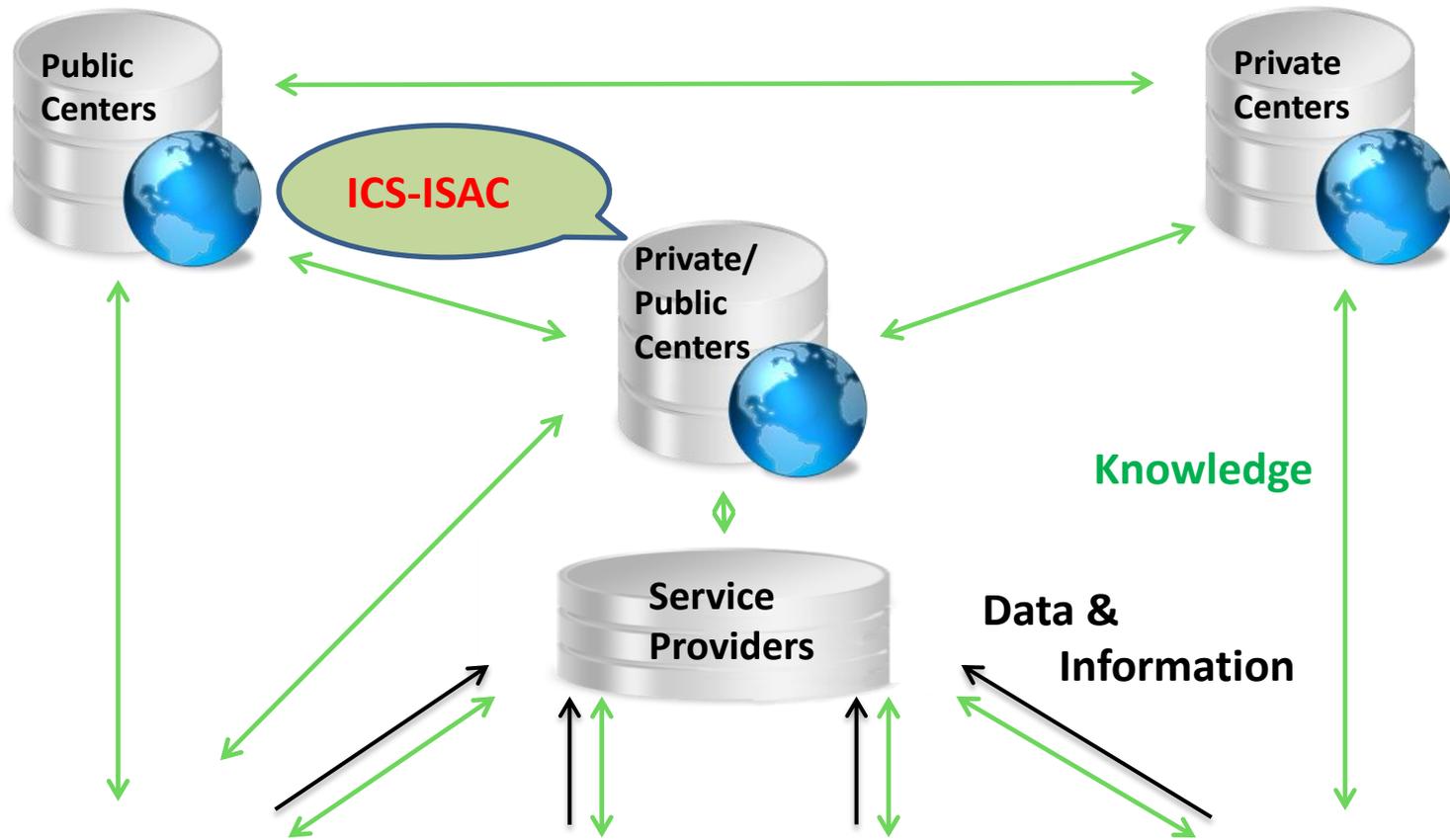
- Continuous Monitoring and Knowledge Sharing
 - Can be implemented with existing technologies
 - Does not introduce excessive cost or risk
 - Possible to achieve in time available
- Robust Self-learning Network
 - Open Architecture
 - Active protection in the face of active threats

Data, Information and Knowledge

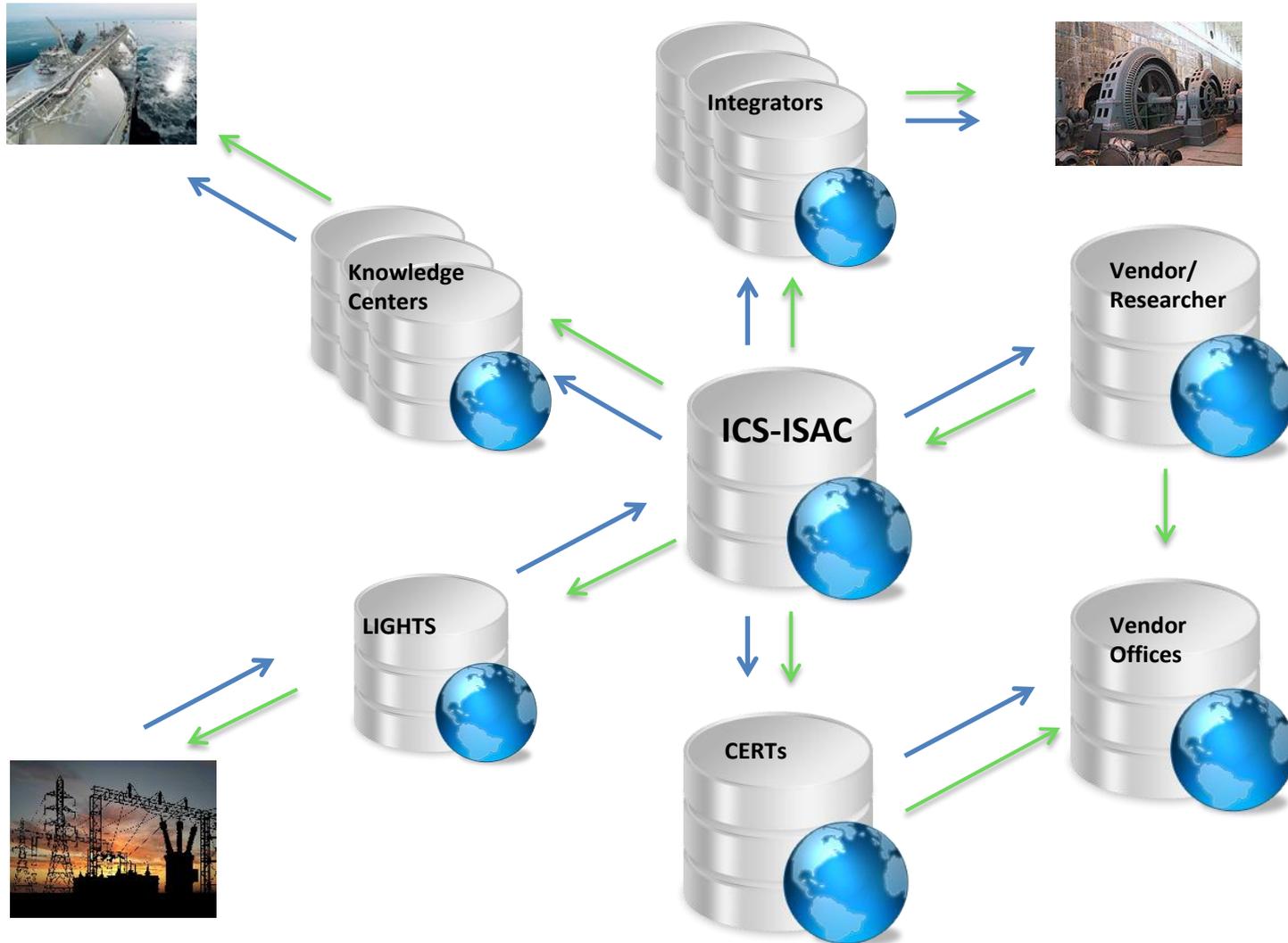
- Data: Items Specific to Devices and Sites
 - Syslog, IDS alert, other atomic unit
- Information: Aggregated Data
 - Incident mangement
- Knowledge: Actionable Sharable Intelligence
 - In control of sharing party



Global Knowledge Network



Real Time Knowledge Sharing



Demonstration

- Knowledge Record entered into ICS-ISAC database
- Database searched for members who have expressed interest in this type of knowledge
- Selected method of sharing is determined
- Knowledge Record transferred to the Member
- Member's systems receive Record and implement monitoring rules



Discussion

- Knowledge Sharing Modes
 - Generic
 - Case Specific (i.e. Researcher/Asset Owner)
- Knowledge Feedback
 - Amplifies the value of initial knowledge
- Other Points?

Take Aways

- Sharing *Information* Can Be Hard
 - Sharing *Knowledge* can be easy
- Knowledge is Best When All Sides Share
 - Facilities, integrators, vendors, researchers
- Remediation is not Protection
 - Survivability is the only goal

