



**TEXAS  
REGIONAL  
ENTITY™**

*An Independent Division of ERCOT*

# Insider Threat

Christopher Humphreys  
CIP Manager

# Physical Security

- **Guns, Gates and Guards**
- **Background Checks**
  - Potential Hires
  - Visitors
- **Physical Access control**
  - Activating/De-activating Badges

# Virtual Security

- **Access Control**
  - Accounts
- **Information Technology**
  - Firewall Configurations
  - Server Security
  - Supervisory Control and Data Acquisition (SCADA)
  - Application Software
    - Direct Grid Interface

# Insider Threat

- **An insider would have access around *both* physical and virtual security perimeters.**
- **What could you or the person sitting next to you accomplish with complete physical and virtual access?**

# Insider Motive

- **Financial Gain**
- **Disgruntled Employee**
  - CAL ISO Incident April 15, 2007
    - Fired contractor whose access was not terminated
    - Pushed emergency electricity shut-off button
      - ◆ Blacked out CAL ISO building, a Sacramento Suburb, and crashed computers
      - ◆ Had the incident occurred during peak grid hours, it could have impacted the entire western grid

# Insider Motive (continued)

- **Espionage**

- Nation States

- Infrastructure information has been posted on various nation state sponsored blogs and websites
- Lack of International Cyber Law
  - ◆ In many countries hacking is not illegal
- Background Investigations
  - ◆ Determine nation state affiliations
  - ◆ Criminal backgrounds

# Insider Threat

- **Insider Threat is now the #1 priority for the Department of Homeland Security's (DHS) CIP Program**
  - The National Infrastructure Advisory Council (NIAC)
    - DHS Presidential-level Advisory Council
    - Conducted "The Insider Threat to Critical Infrastructures" - April 8<sup>th</sup> 2008

# Insider Threat

- **Insider Threat Policy Recommendations from NIAC Study:**
  - Education and Awareness
  - Employee Screening
  - Technology Policy
  - Information Sharing



**TEXAS  
REGIONAL  
ENTITY™**

*An Independent Division of ERCOT*

Questions?

