Southern California Edison Cybersecurity

Richard E Pace
Program Manager
Cybersecurity Incident Response

Energy for What's Ahead℠

SOUTHERN CALIFORNIA EDISON®

SCE Cybersecurity

- Consists of Operations Center, Engineering, Risk and Governance, Awareness, and Outreach
- Responsible for security of grid control systems, data centers, employee devices (laptops and phones), network, any other technologies that access or connect to SCE

SCE's Cybersecurity Threat Landscape

- Nation states
- Opportunistic groups or individuals ("hackers")
  - Ransomware
  - Financial data compromise
  - Credential harvesting
  - Any other way to make money

Threat and Intelligence Sharing

- Cybersecurity intelligence is extensively shared not only in the utility space, but across differing businesses to ensure the widest protection across the US and our allies
  - Indicators of compromise (IOC)
  - Intelligence reports
- We work closely with local and national FBI offices, DHS, DoE, and multiple other federal and state government agencies
- We share intelligence with other utilities in California, the Western US, and nationwide through multiple channels
- Contracts with cybersecurity vendors to provide us with their intelligence

Internal and External Coordination and Integration

- Projects and programs across the company – IT, Transmission & Distribution, Generation, Energy Trading, Customer Service, Finance, HR, etc.
- Multiple exercises annually to continually train our response personnel
  - Internal
    - Small scale for individual parts of the business
    - Large scale to incorporate entire corporation from executives on down
  - External
    - GridEx – nationwide utility exercise with 250+ companies
    - U.S. Government exercises – Department of Energy, Department of Homeland Security, FBI, Department of Defense