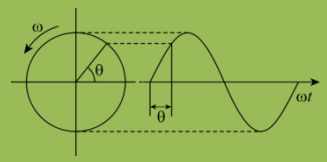
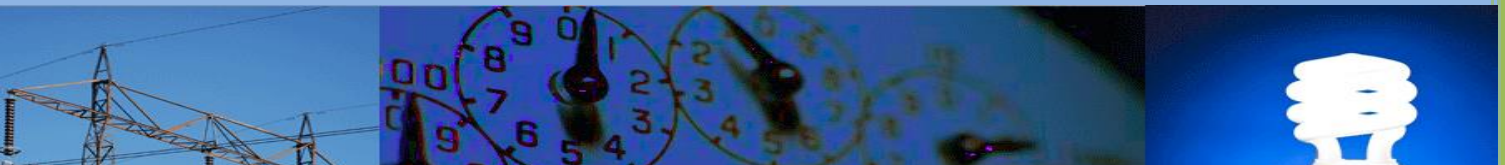
Utilicast

Understanding the Perils of our Power Grid Security



Dawn or Doom 2016



October 4th 2016

Ukraine Grid Attack

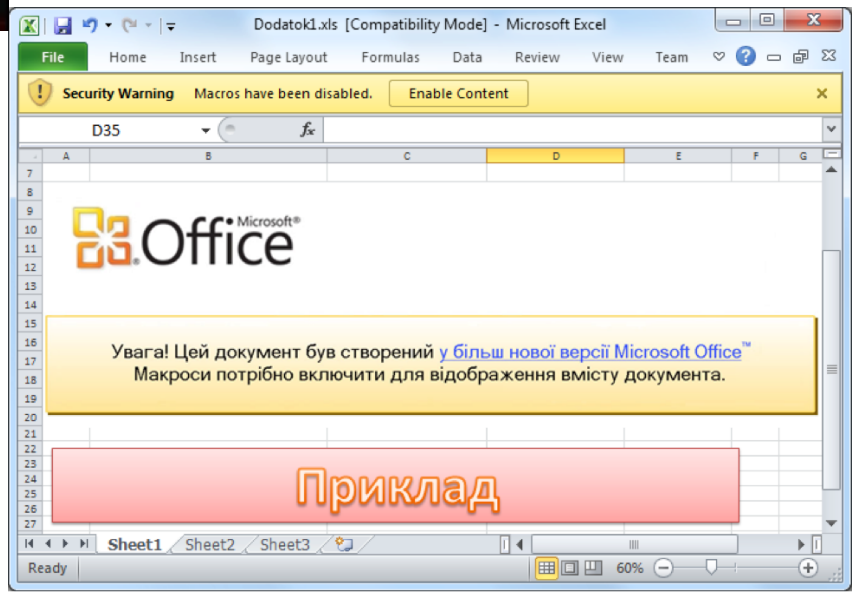
1) Spear phishing to gain access to business network

2) Theft of credentials to control center network

3) Remote admin to open breakers

4) Wipe hard drives of operator computers

5) Jam call center phone lines



http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf

Aurora Vulnerability

2007 Idaho National Laboratory Experiment

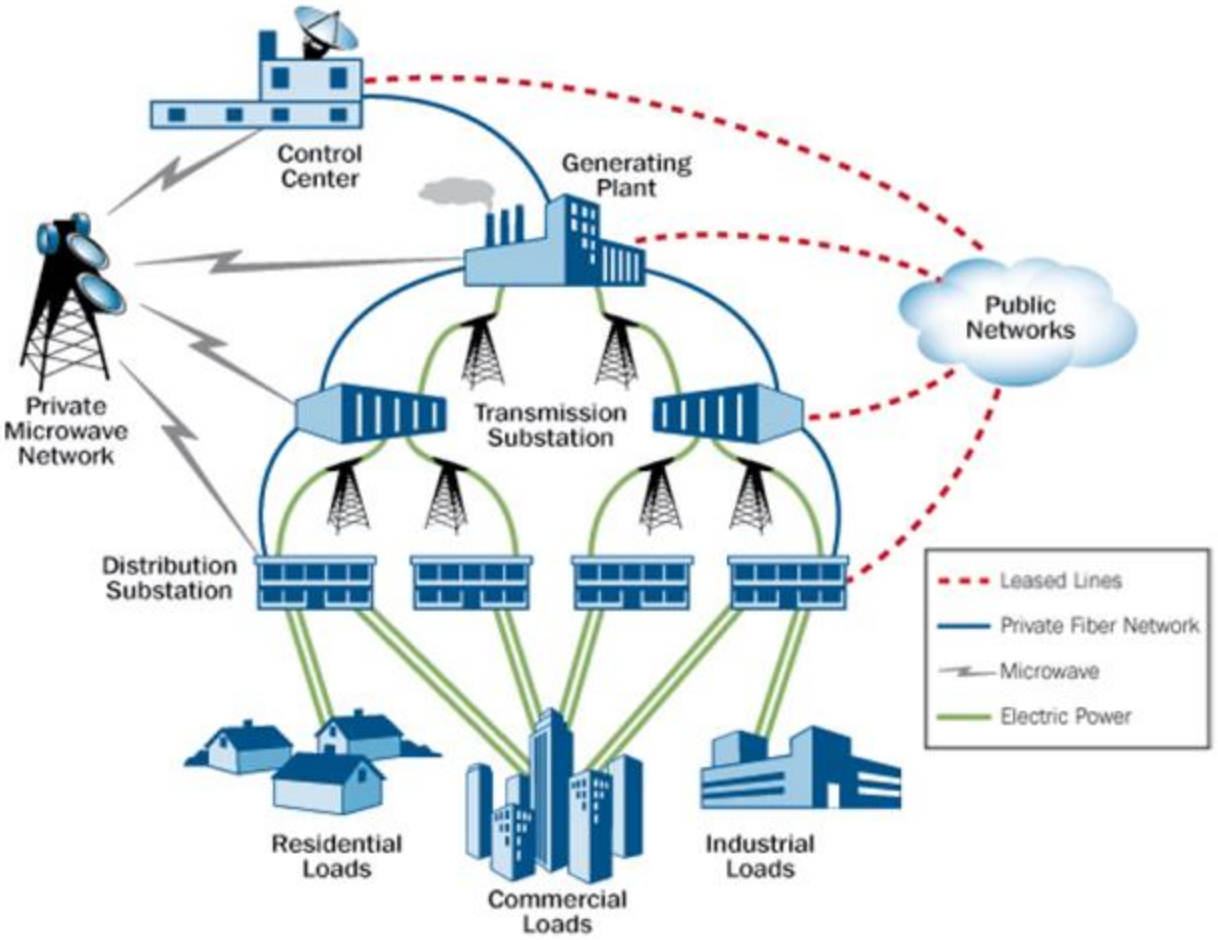
- *Open and close breakers in rapid succession*

Questions to Consider

- *Is it possible to hack the U.S. power grid?*
- *Why are these systems all connected?*
- *Is mandatory compliance with security standards enough?*
- *How likely is our grid to be attacked?*
- *Should I ever click on a link again?*

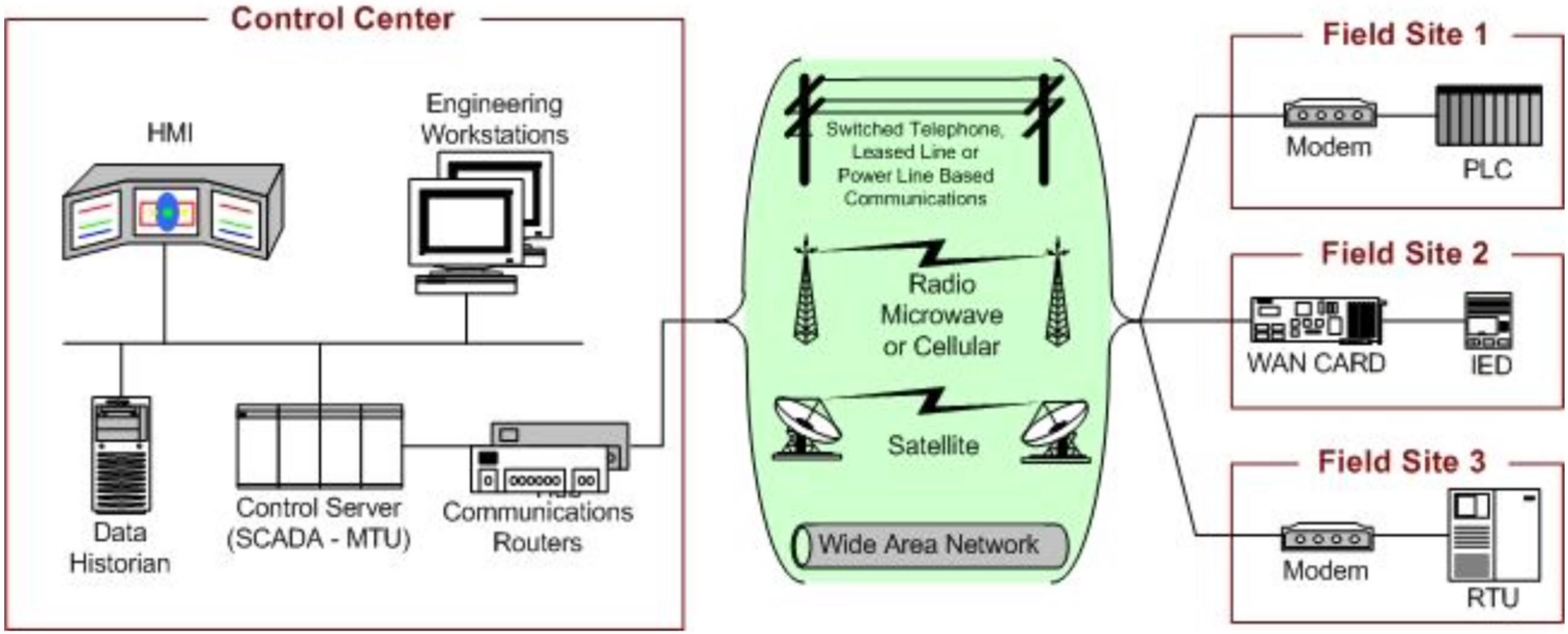
Grid Components

How Power Gets to You



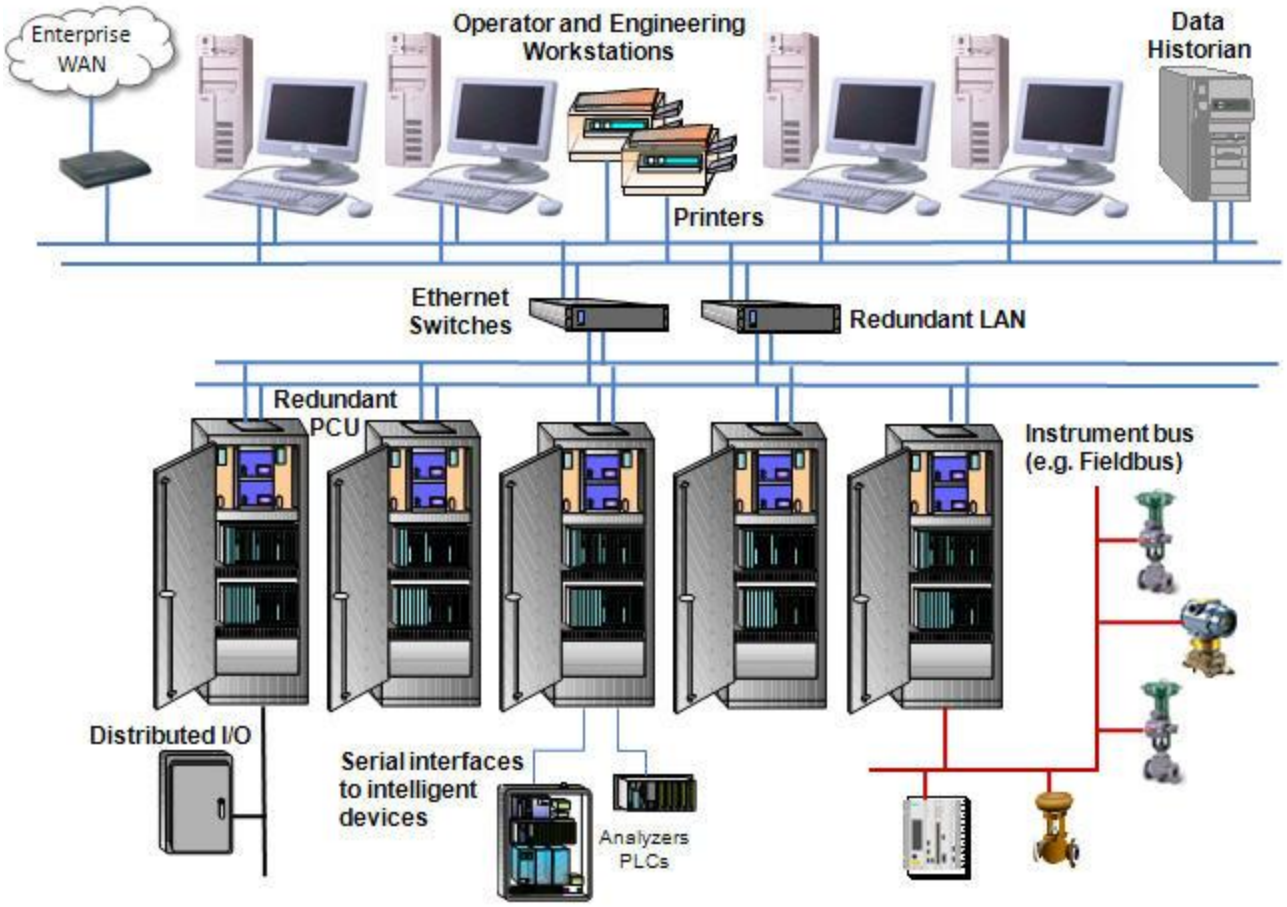
http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/Energy_SSP_2010.pdf

SCADA / ICS



http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Distributed Control System

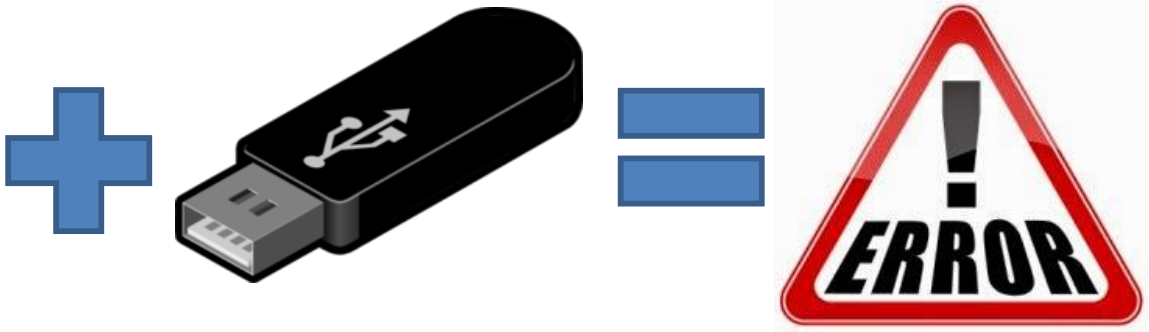


http://www.industryconsulting.org/dcsscada1.htm

Air Gap the SCADA network?

- *Air-gap refers to computers or networks that are not connected directly to the internet or to any other computers that are connected to the internet (Wired Magazine)*

- *Enter Stuxnet:*



Why Connect Anyway?

- *Neighboring Utilities, Regional Reliability Coordinators need data for situational awareness*
- *Metering data is used for energy accounting*
- *Remote administration allows for fast response from a limited number of experts*
- *Connection to market systems allows dispatch across a wider pool of generators(including renewables)*

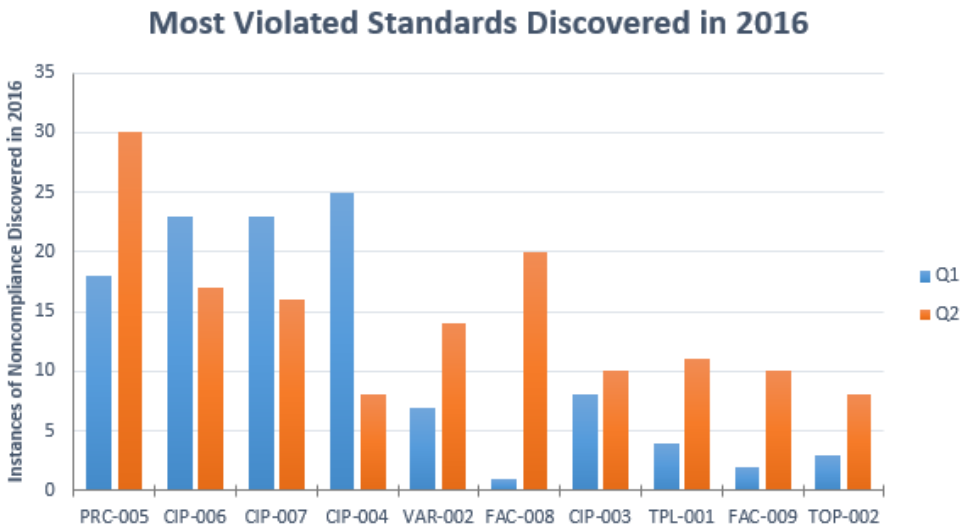
&

Protection Resources

- *DOE – Department of Energy*
  - *Risk Management*
  - *Incident Response*
- *ICS-CERT – Industrial Control Systems Cyber Emergency Response Team*
  - *Division of the Department of Homeland Security*
  - *Information Sharing*
  - *Connection to law enforcement*
- *NERC – North American Electric Reliability Corporation*
  - *Granted authority by FERC – Federal Energy Regulatory Commission*
  - *Critical Infrastructure Protection standards*

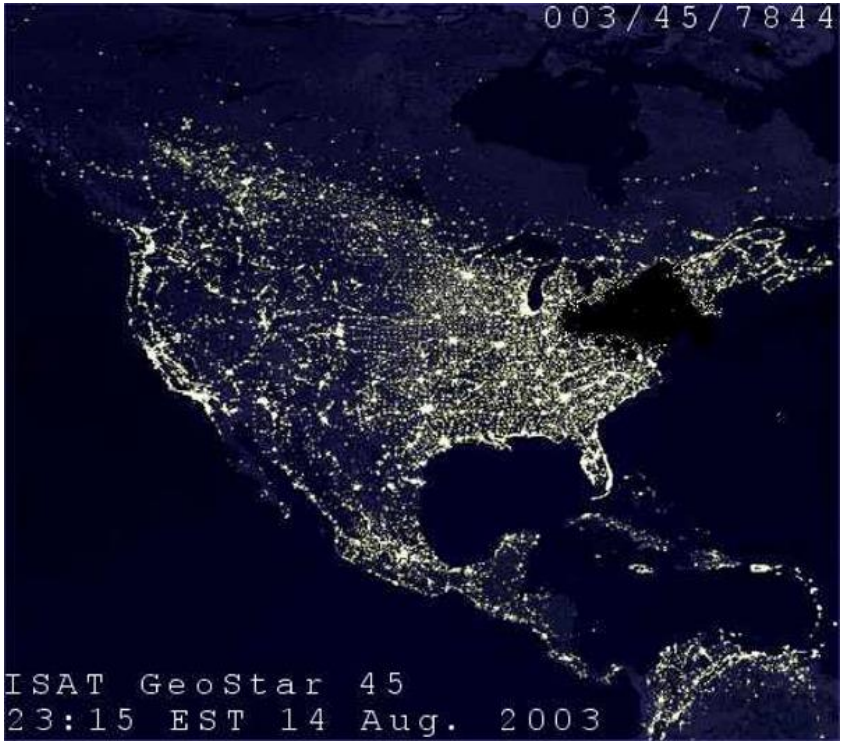
NERC CIP

- *Mandatory standards to protect the bulk power system against cybersecurity compromises that could lead to misoperation or instability*
- *Fines for non-compliance up to $1M per day per violation*



- *Companies spend more on compliance programs than the fines levied against them*

August 14, 2003 Blackout



- *50 million people without power*
- *Loss of 61,800 MW of electric load*
- *Power out for up to 2 days*
- *Total economic loss ~$7 billion to $14 billion*

- *Energy Policy Act of 2005*
  - *Results in NERC standards becoming mandatory and enforceable*

Current Protections

- *BES Cyber System Categorization*
- *Security Management Controls*
- *Personnel & Training*
- *Electronic Security Perimeters*
- *Physical Security*
- *System Security Management*
- *Incident Reporting and Response Planning*
- *Recovery Plans for BES Cyber Systems*
- *Configuration Change Management and Vulnerability Assessments*
- *Information Protection*

Standards Development

- *CIP version 5 / version 6 (currently in force)*
  - *First Draft Completed by Standards Drafting Team: 12/16/11*
  - *Approved by NERC: 11/26/12*
  - *Ordered by FERC: 11/22/13*
  - *In effect: 7/1/16*

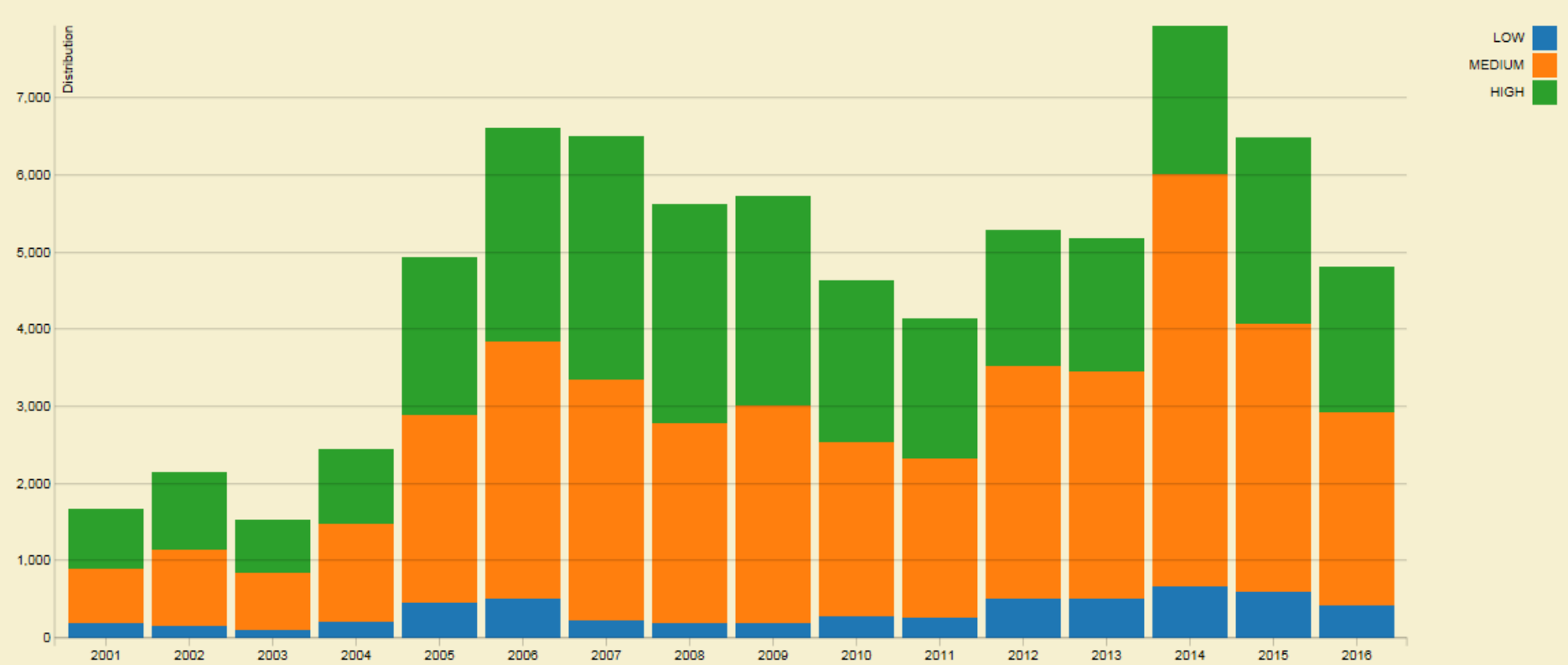
Rate of New Vulnerabilities

Sponsored by DHS/NCCIC/US-CERT

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

NIST National Institute of Standards and Technology



https://nvd.nist.gov/visualizations/cvss-severity-distribution-over-time

Compliance vs. Security

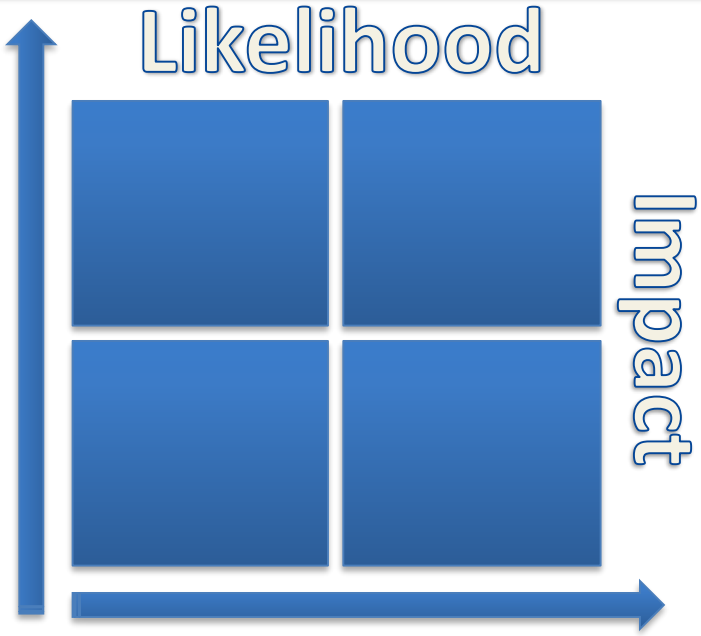
- *"We fear the auditor more than the hacker"*
- *Audits occur every 3 years*
- *Getting hacked is a risk, but not a guarantee*
- *Compliance carries the burden of proof, Security carries the burden of protection*
  - *Ex: Visitor logs in a physical security perimeter*
- *Compliance should be the floor of the Security program, not the ceiling*

Limits of NERC CIP Scope

- *Bulk Electric System only (the big wires)*
- *Limited to cyber systems which could have a negative impact in real time (within 15 minutes)*
- *No protections required for corporate networks, including 3rd party connections*
- *No protections required for front-end market systems*

Other Reliability Risks

- *Physical attack*
- *Electromagnetic Pulse (EMP)*
- *Human error*



- *Natural disasters and extreme weather conditions*
- *Equipment failure and aging infrastructure*

Regulation isn't free

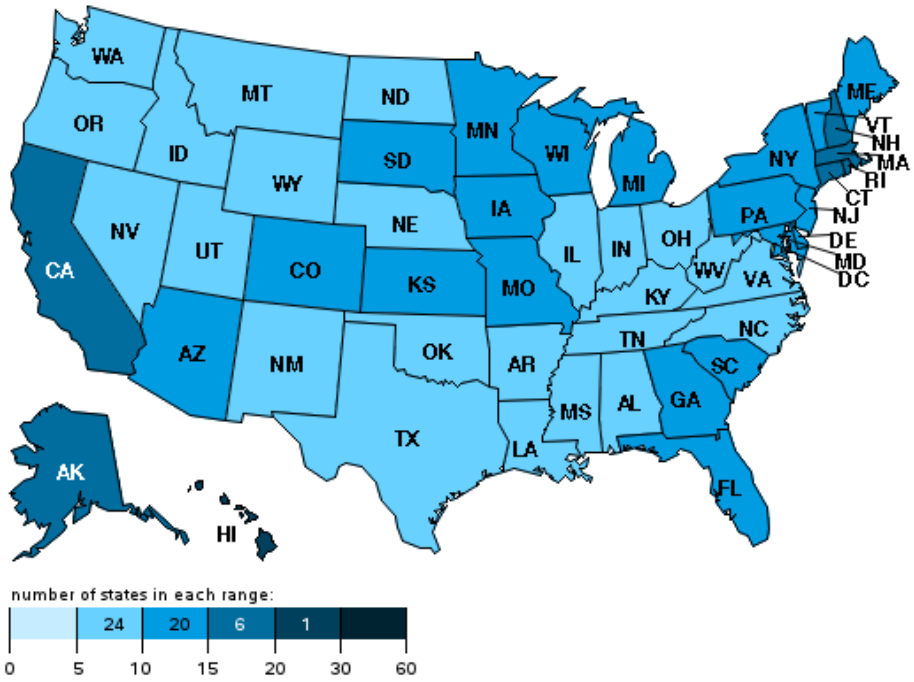
Cybersecurity spending on power grid infrastructure to reach nearly $3 billion

05/24/2013 By Editors of Electric Light & Power/ POWERGRID International

Global spending on cybersecurity solutions to safeguard the electrical grid infrastructure is anticipated to reach $2.9 billion by the end of 2013, according to a new report from ABI Research.

U.S. electric industry average revenue per kilowatthour
June 2016, cents per kilowatthour

eia

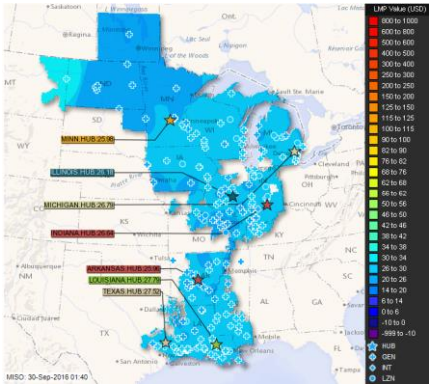


Threat Sources

- *Nation States*
- *Anarchists*
- *Disgruntled employees*
- *Non-sector specific attack*
- *Profit motive is limited*

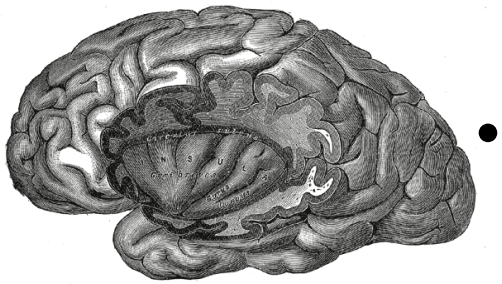
Emerging Trends

- *Increased connectedness!*
  - *Inter-utility for situational awareness*
  - *Intra-utility as technologies reach end of life*
  - *Mergers and acquisitions*



- *Electricity markets*
  - *Forward markets & real time markets depend on data*
  - *Recent market launches in mid-South and West Coast*
- *Smart Grid technologies*
  - *Advanced Metering Infrastructure (AMI)*
  - *Distributed Energy Resources (DER)*

Potential Solutions



- *Greater security awareness of our people*
- *Additional preventative controls & technologies*
- *Faster, more automated incident response*
- *Microgrids*

- *Other Solutions?*

Questions


?
Utilicast
Chris Unton
P.O. Box 38
Kirkland, WA 98083
tel: 866.243.2650
fax: 866.424.6132
cell: 317.690.4599
crunton@utilicast.com