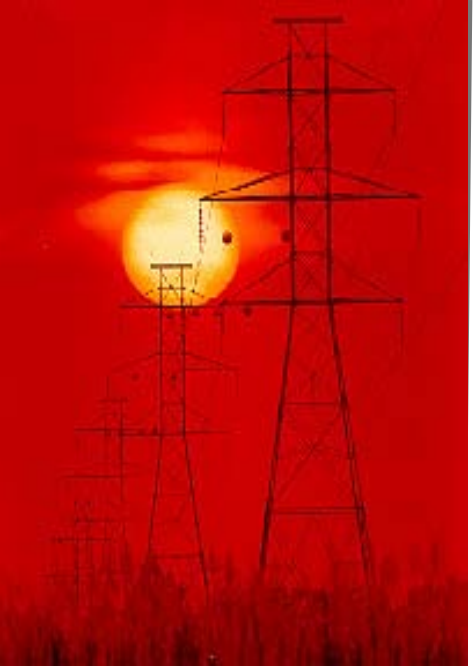


California Public Utilities Commission

Smart Grid Symposium

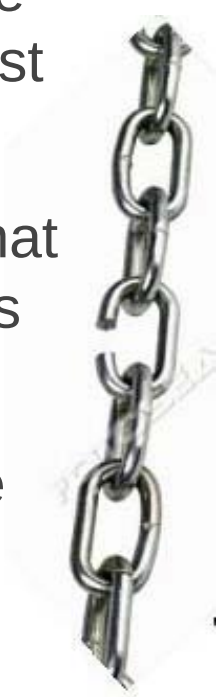
Cyber Security and Smart Grid

Frances Cleveland

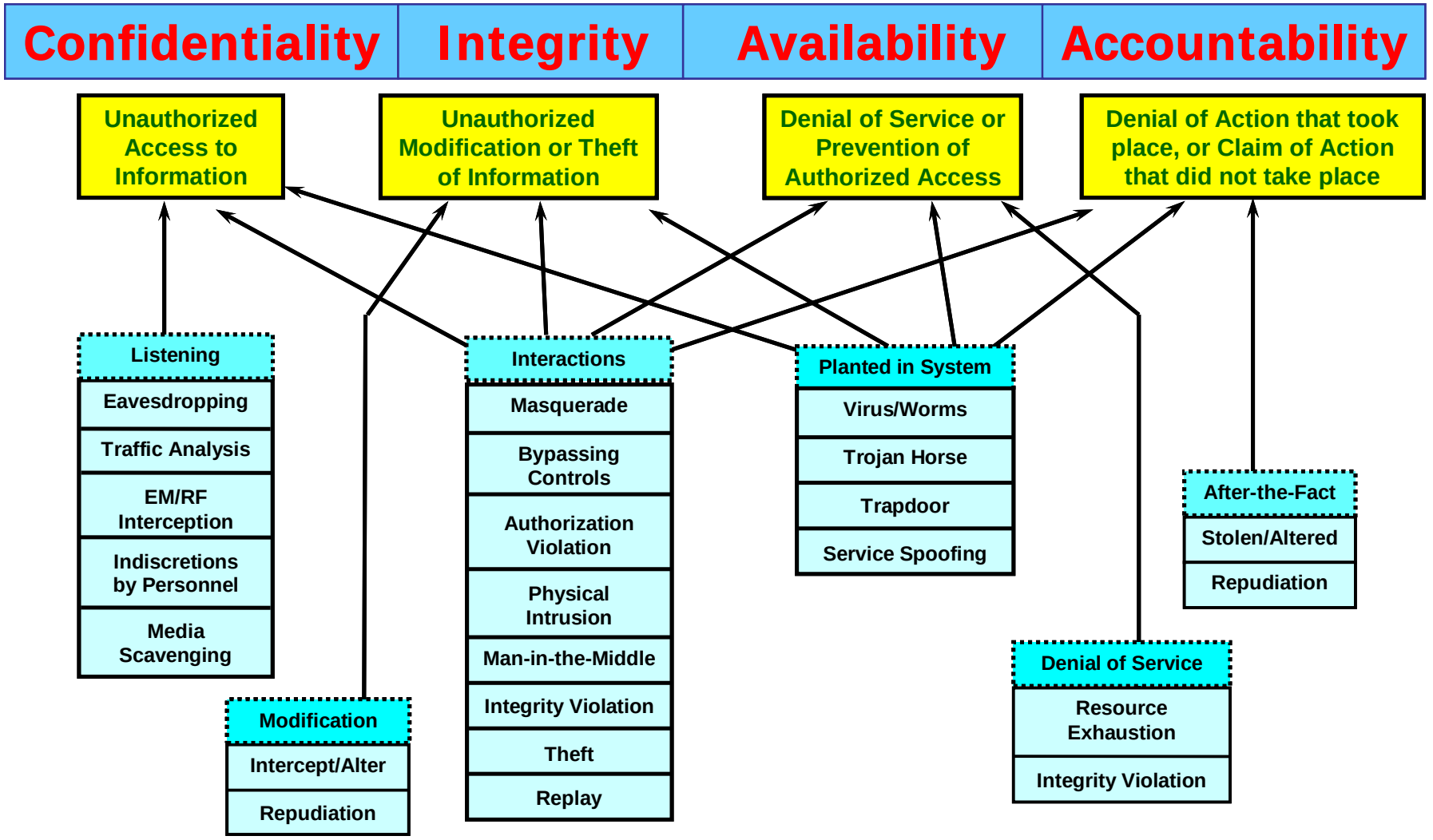
Xanthus
Consulting International

What is Security? Key Take-Aways

1. Encryption, by itself, does not provide security. Security requires many different solutions.
2. Security threat agents can undertake deliberate attacks OR cause inadvertent events.
3. The most dangerous “attacker” is a disgruntled employee who knows exactly where the weaknesses are the easiest to breach and could cause the worst damage.
4. Security solutions must be end-to-end and layered, so that if one layer is breached, the next will be there. Security is only as strong as its weakest link.
5. Security will ALWAYS be breached at some time – there is no perfect security solution.



1. Encryption, by itself, does not solve all security threats – there are so many different types of threats!



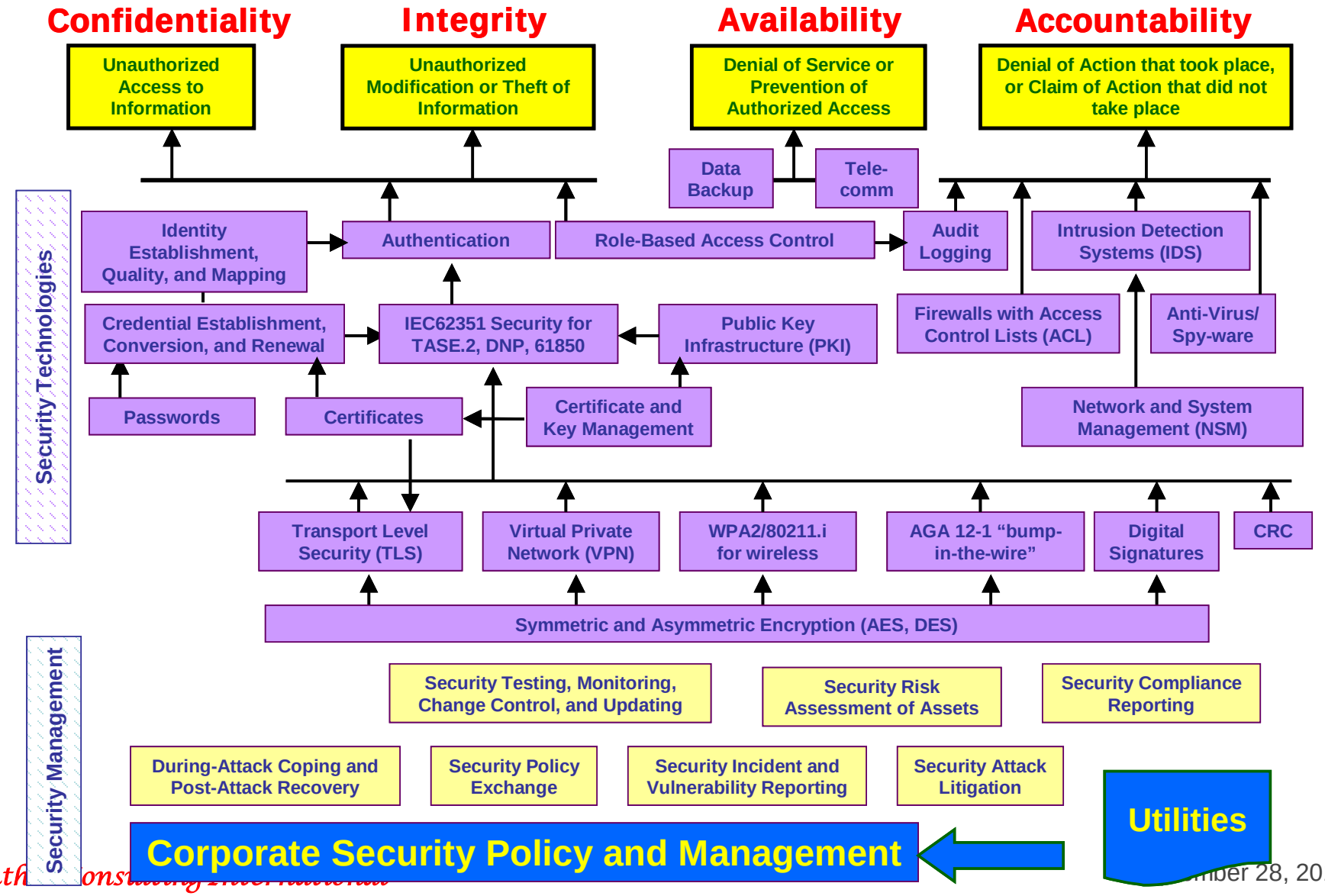
2. Security Threat Agents may undertake deliberate attacks or cause inadvertent events

- **Inadvertent**: Threat Agents which may cause inadvertent "attacks" on systems
  - Careless users
  - Employees who bypass security
  - Safety system failures
  - Equipment Failures
  - Natural Disasters
- **Deliberate**: Threat Agents which undertake deliberate attacks
  - Disgruntled Employee
  - Industrial Espionage Agents
  - Vandals
  - Cyber Hackers
  - Viruses and Worms
  - Thieves
  - Terrorists

3. The greatest security threat (agent) is ?

- Terrorist
- Internet hacker
- Hurricanes
- Careless mistakes
- Disgruntled employee
- Belief in security by obscurity
- Industrial spy

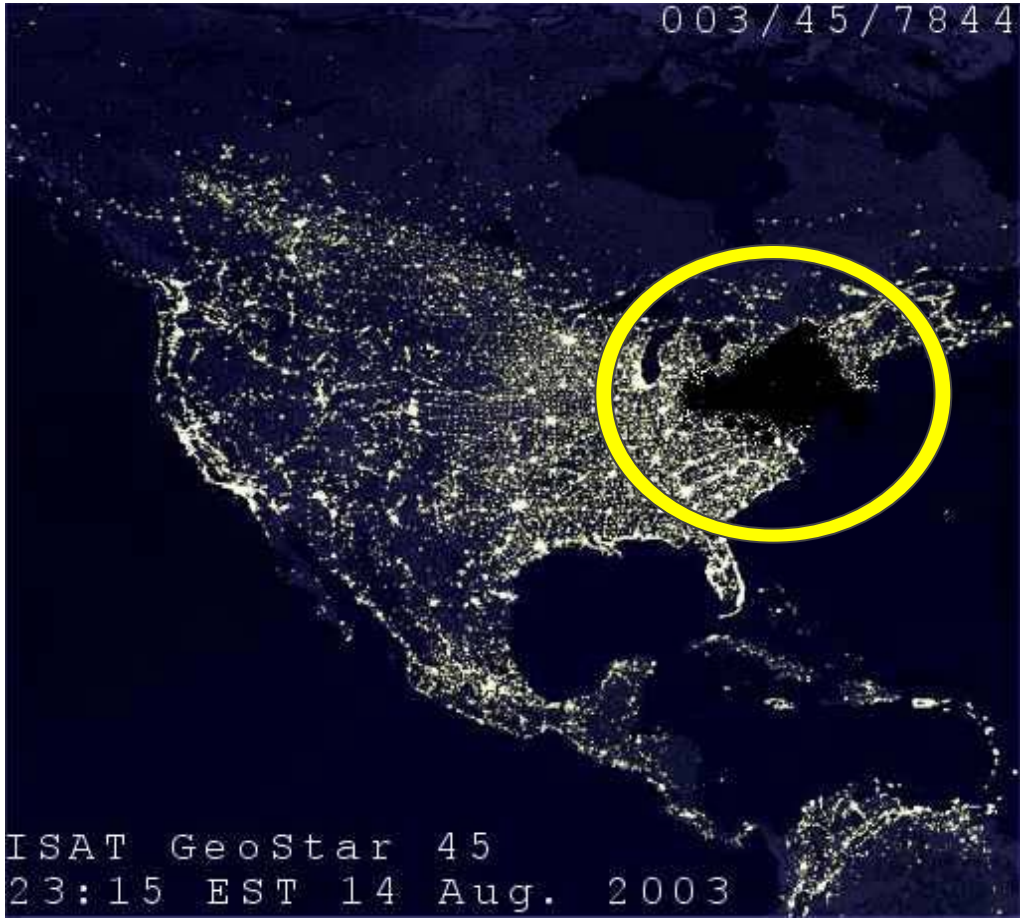
4. Security solutions must be end-to-end and layered, so that if one layer is breached, the next will be there



5. Security will ALWAYS be breached at some time – there is no perfect security solution.

- **Deterrence and delay**, to try to avoid attacks or at least delay them long enough for counter actions to be undertaken. This is the primary defense, but should not be viewed as the only defense.
- **Detection of attacks**, primarily those that were not deterred, but could include attempts at attacks. Detection is crucial to any other security measures since if an attack is not recognized, little can be done to prevent it. Intrusion detection capabilities can play a large role in this effort.
- **Assessment of attacks**, to determine the nature and severity of the attack. For instance, is the entry of a number of wrong passwords just someone forgetting or is it a deliberate attempt by an attacker to guess some likely passwords?
- **Communication and notification**, so that the appropriate authorities and/or computer systems can be made aware of the security attack in a timely manner. Network and system management can play a large role in this effort.
- **Response to attacks**, which includes actions by the appropriate authorities and computer systems to mitigate the effect of the attack in a timely manner. This response can then deter or delay a subsequent attack.

Cyber Security and the Smart Grid – Why is it important?



What is this picture?

August 14, 2003 Blackout – Northeastern United States

What caused the blackout?

- ☑ Power Equipment Failures?
- ☑ Software Application Failures?
- ☑ Information Flow Design Flaws?

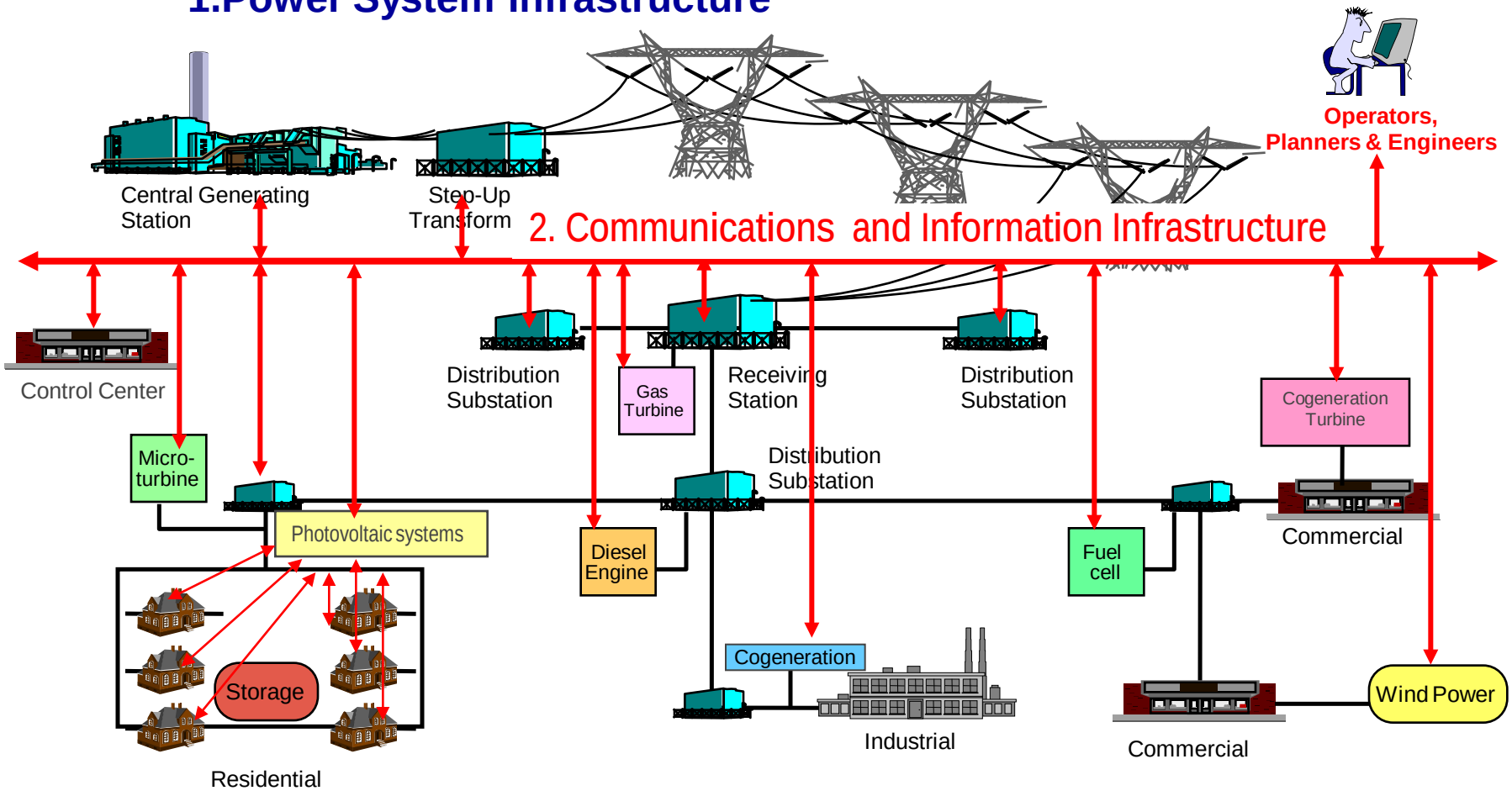
What does August 2003 have to do with Security? And Information Flow Design Flaws? Are those Smart Grid Security Issues?

Yes, given how dependent the Smart Grid has (and will increasingly) become on information, security for "All Hazards" includes the need for a reliable, secure information infrastructure

Need to manage both the Power System Infrastructure and the Information Infrastructure

Network and System Management with Intrusion Detection is the "SCADA system" for the information infrastructure

1.Power System Infrastructure

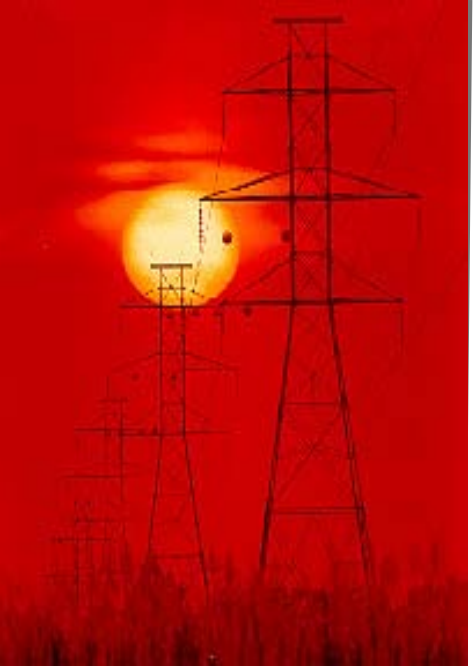


Given all these activities, How should Stakeholders – Particularly Regulators – Approach Security?

- **Utilities:** Define and specify **security requirements, based on the assessment of business processes, as intrinsic** to any new or upgraded systems, as well as retrofits.
- **Security Standards Groups:** Look to the power industry and other industries for security requirements as input to standards – **one size does not fit all**
- **Vendors:** Implement security as flexible to meet varying needs, but also as **fully integrated capabilities right from initial design** in all products and systems
- **Customers: Demand security**, with proof and oversight – no unauthorized personnel accessing private customer information
- **Regulators:** Understand the issues raised by Smart Grid interoperability requirements, the need for interoperability standards, and the **need to implement sometimes costly security measures to avoid serious future security problems.**
- **NIST Interim Roadmap:** Input to the NIST cyber security standards efforts by regulators and other stakeholders would be very appreciated.

Regulator Responses to Cyber Security?

- From NARUC/FERC Smart Grid Collaborative proposed funding criteria for projects:
  - *How the project will address cyber security issues and ensure that it maintains compliance with Federal Energy Regulatory Commission-approved reliability standards during and after the installation of Smart Grid technologies, [covering **privacy**, **integrity** of data, **authentication** of communications, **unauthorized use or modification** of devices, and **physical** protection]*
- Possibly add:
  - Require security policies, security training (and retraining), and enforcement
  - Require measures to ameliorate denial of service
  - Extend security requirements to all power system areas, including transmission, distribution, customer interfaces, distributed energy resources, and third party access
  - Include within security the management of the information infrastructure that supports the Smart Grid.



Questions? Comments?