NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Grid Security & NERC

Janet Sena, Senior Vice President, Policy and External Affairs
Southern States Energy Board 2017 Associate Members Winter Meeting
February 27, 2017

RELIABILITY | ACCOUNTABILITY




Recent NERC History

Energy Policy Act of 2005 – Section 215 Federal Power Act

- Authorized creation of the Electric Reliability Organization (ERO)
  - Interconnected grid called for North American approach
  - Reliability standards developed by ERO
  - Oversight by U.S. and Canadian authorities
  - Mandatory and enforceable by all users, owners and operators of the **bulk power system** – includes **cyber security protection**
  - Mandate to assess reliability

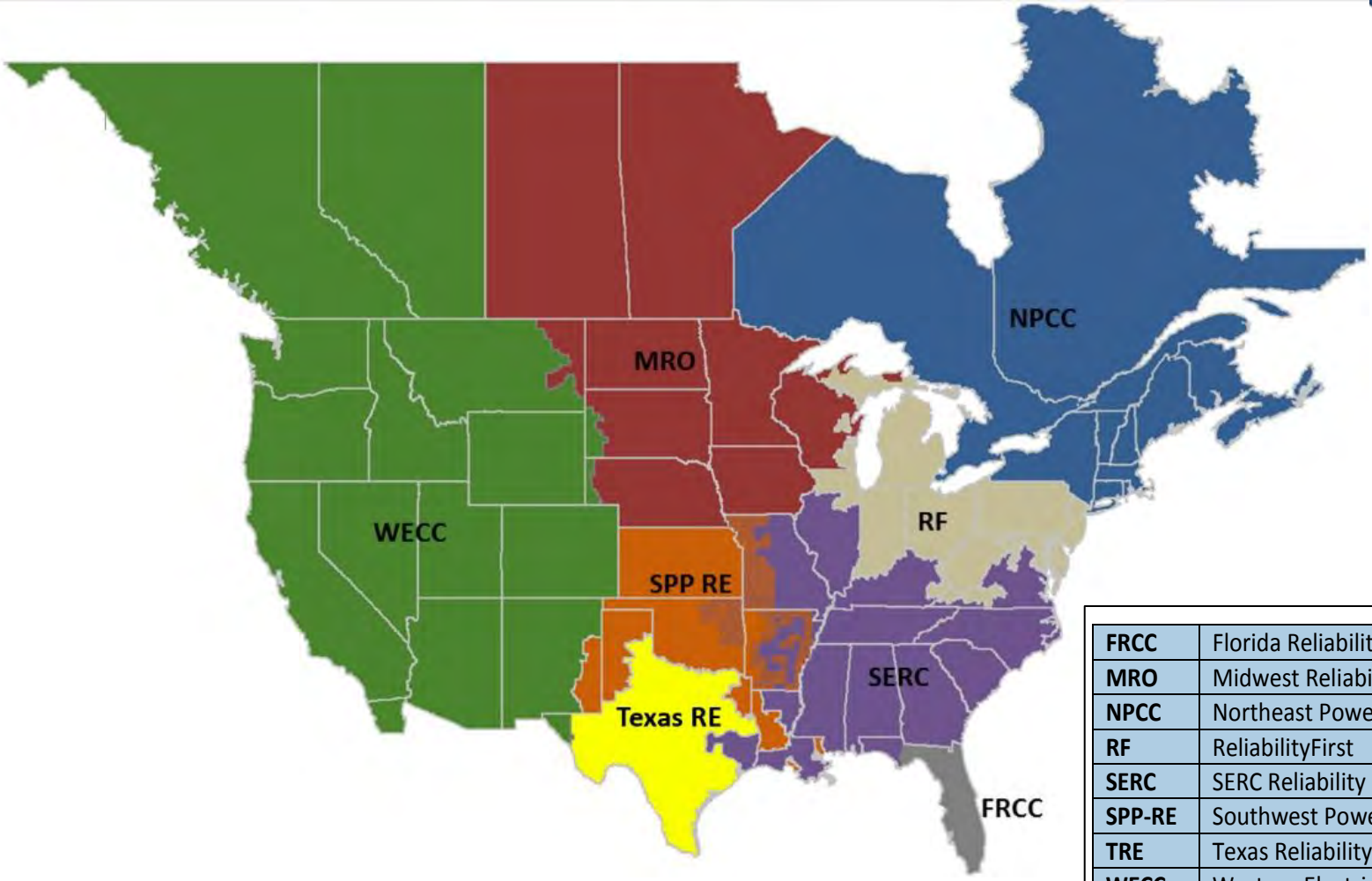
Recent NERC History

- 2006 – North American Electric Reliability Corporation (NERC) certified by the Federal Energy Regulatory Commission (FERC) as the ERO
- 2007 – First standards become mandatory and enforceable
- 2008 – FERC approved eight reliability standards that NERC developed related to critical infrastructure protection (the "CIP Standards")

Unique Form of Regulation

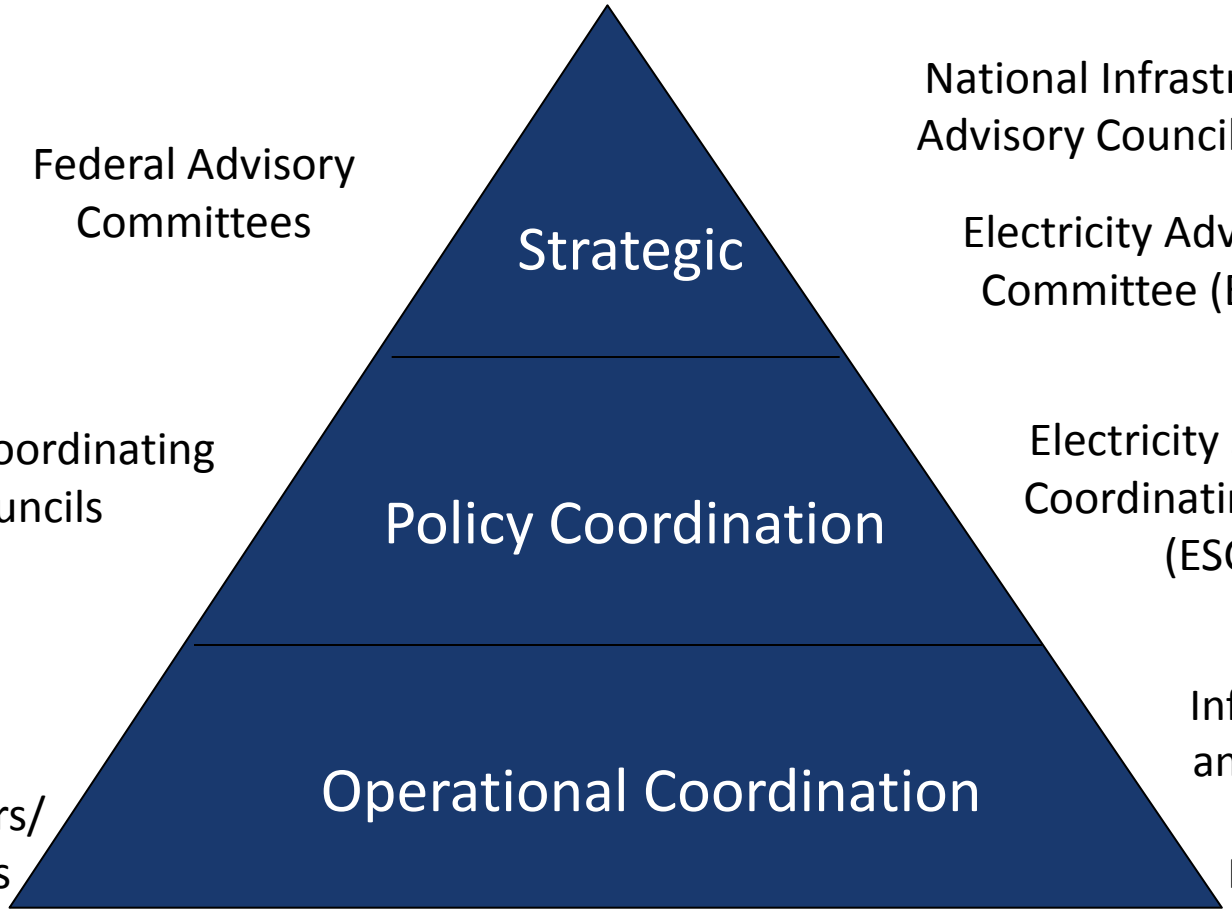
- Interconnected grid with Canada; oversight by U.S. and Canadian authorities
- Roughly 1,500 owners, operators, and users of the bulk power system (BPS)
  - Focus on reliable operation of the BPS
  - Standards cannot require construction of new transmission or generation capacity
- Independent Board of Trustees (Board)
- All entities with a material interest in the reliability of the BPS can be NERC members
- Member Representatives Committee reports to the Board
- Eight Regional entities at the front line, performing delegated functions

NERC Regions



FRCC	Florida Reliability Coordinating Council
MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
SPP-RE	Southwest Power Pool Regional Entity
TRE	Texas Reliability Entity
WECC	Western Electric Coordinating Council

CIP Relationships



Federal Advisory Committees

National Infrastructure Advisory Council (NIAC)

Electricity Advisory Committee (EAC)

Sector Coordinating Councils

Electricity Subsector Coordinating Council (ESCC)

Information Sharing and Analysis Centers/ Organizations

Electricity Information Sharing and Analysis Center (E-ISAC)
NERC Standards

Cyber Security Standards

- Designed to provide a foundation of sound security practices across the BPS
- Mandatory cyber standards cover numerous security aspects
  - Critical assets identified
  - Critical control centers and facilities secured
  - Operations cyber assets fire walled and well patched
- Industry is audited for compliance with the standards
- CIP V5 implementation

Physical Security Standards

- CIP-014 purpose - To **identify** and **protect** transmission stations and transmission substations, their associated primary control centers, that if rendered inoperable or damaged as a result of physical attack could result in widespread instability, uncontrolled separation, or cascading within an interconnection
- Applicability
  - Transmission Owners (TO)
  - Transmission Operators (TOP)
- Effective date – October 1, 2015

E-ISAC: Not Every Vulnerability Requires a Standard

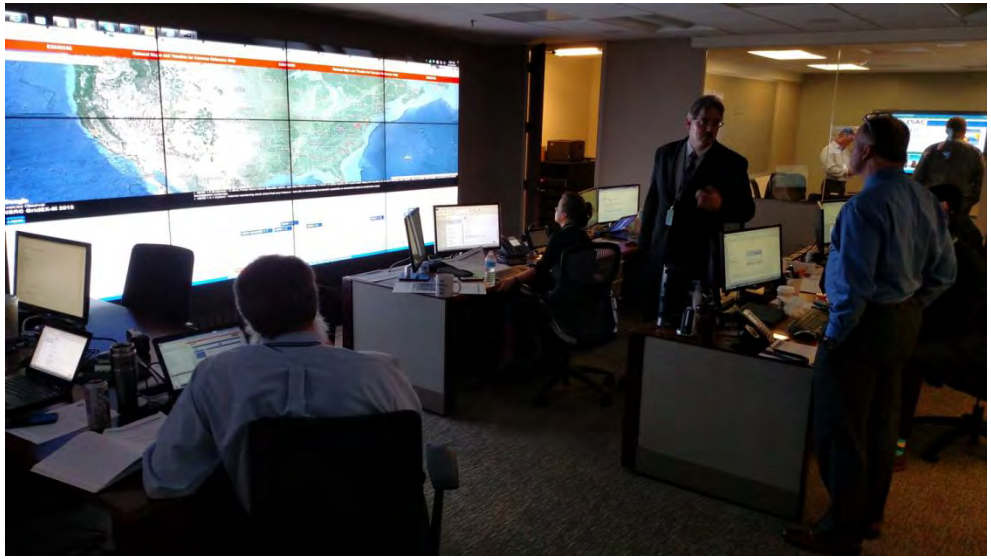
- ISAC concept introduced in Presidential Decision Document 63, published in 1998
  - Electric power was identified as a critical sector along with 14 others
  - Homeland Security Presidential Directive 7 (2003)
  - Presidential Policy Directive 21 (2013)
- Electricity sector's ISAC hosted by NERC since 1998

External Partners

- Public-Private Partnership (ESCC)
- Government
  - Department of Energy (DOE)
  - National Infrastructure Coordinating Center (NICC)
  - National Cybersecurity and Communications Integration Center (NCCIC)
  - Other federal agencies (FBI, DOD, etc.)
- Cross-Sector Partners
  - Other ISACs/ISAOs
  - Private-sector partners

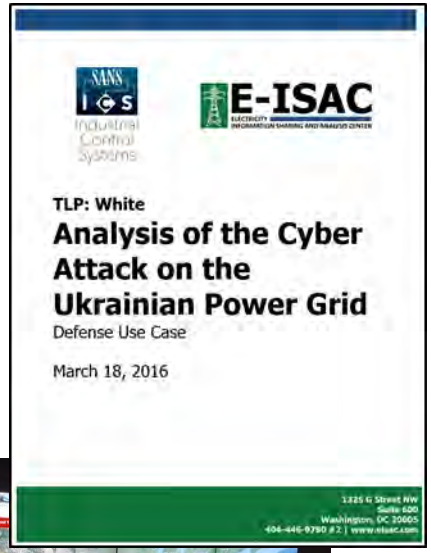
E-ISAC Organization

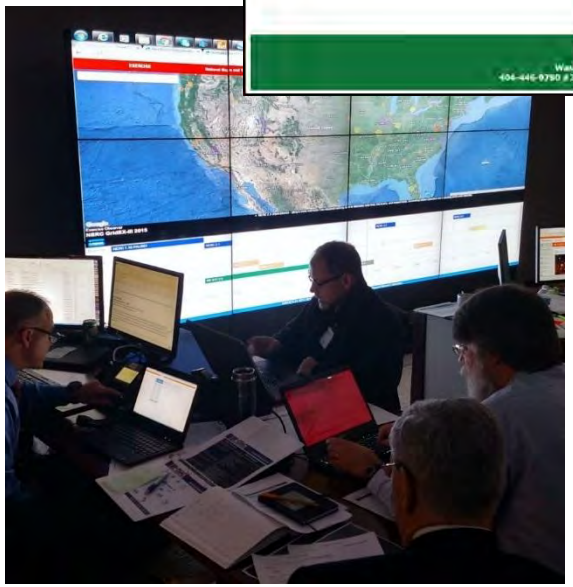
- Watch Operations team
- Cyber Analysis team
- Physical Analysis team
- Programs and Engagement team



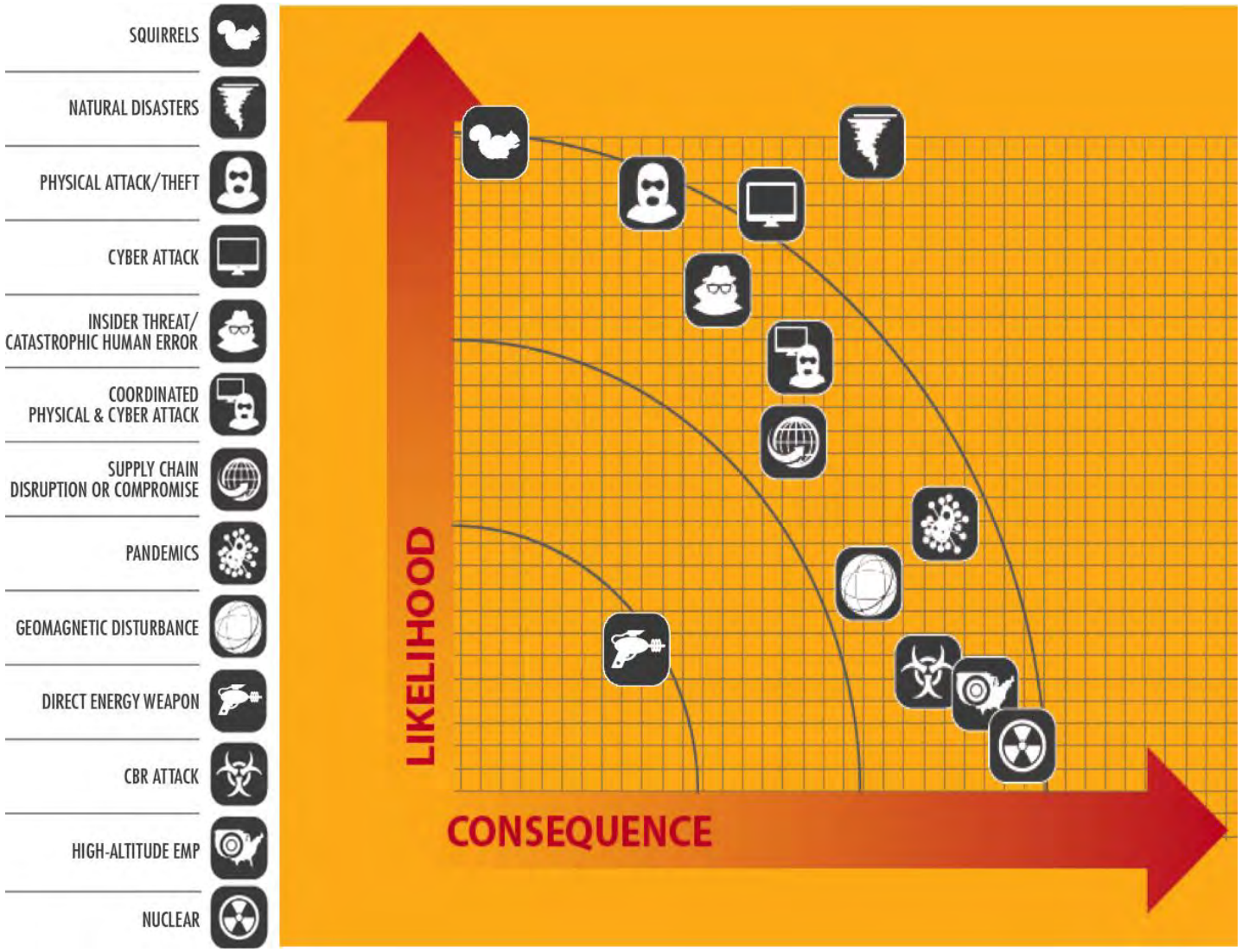
E-ISAC Products and Services

- Products
  - NERC alerts
  - Incident (cyber and physical) bulletins
  - Daily, weekly, and monthly summary reports
  - Issue-specific reports
- Programs and Services
  - Monthly briefing series, first Tuesday of the month
  - Training at quarterly CIPC meetings
  - Grid Security Conference (GridSecCon)
  - Grid Exercise (GridEx)
  - Cybersecurity Risk Information Sharing Program
  - (CRISP)
  - Physical security outreach visits
- Tools
  - E-ISAC portal (www.eisac.com)
  - Emergency notifications
  - STIX/TAXII automated information sharing


SANS ICS Industrial Control Systems
E-ISAC
TLP: White
Analysis of the Cyber Attack on the Ukrainian Power Grid
Defense Use Case
March 18, 2016

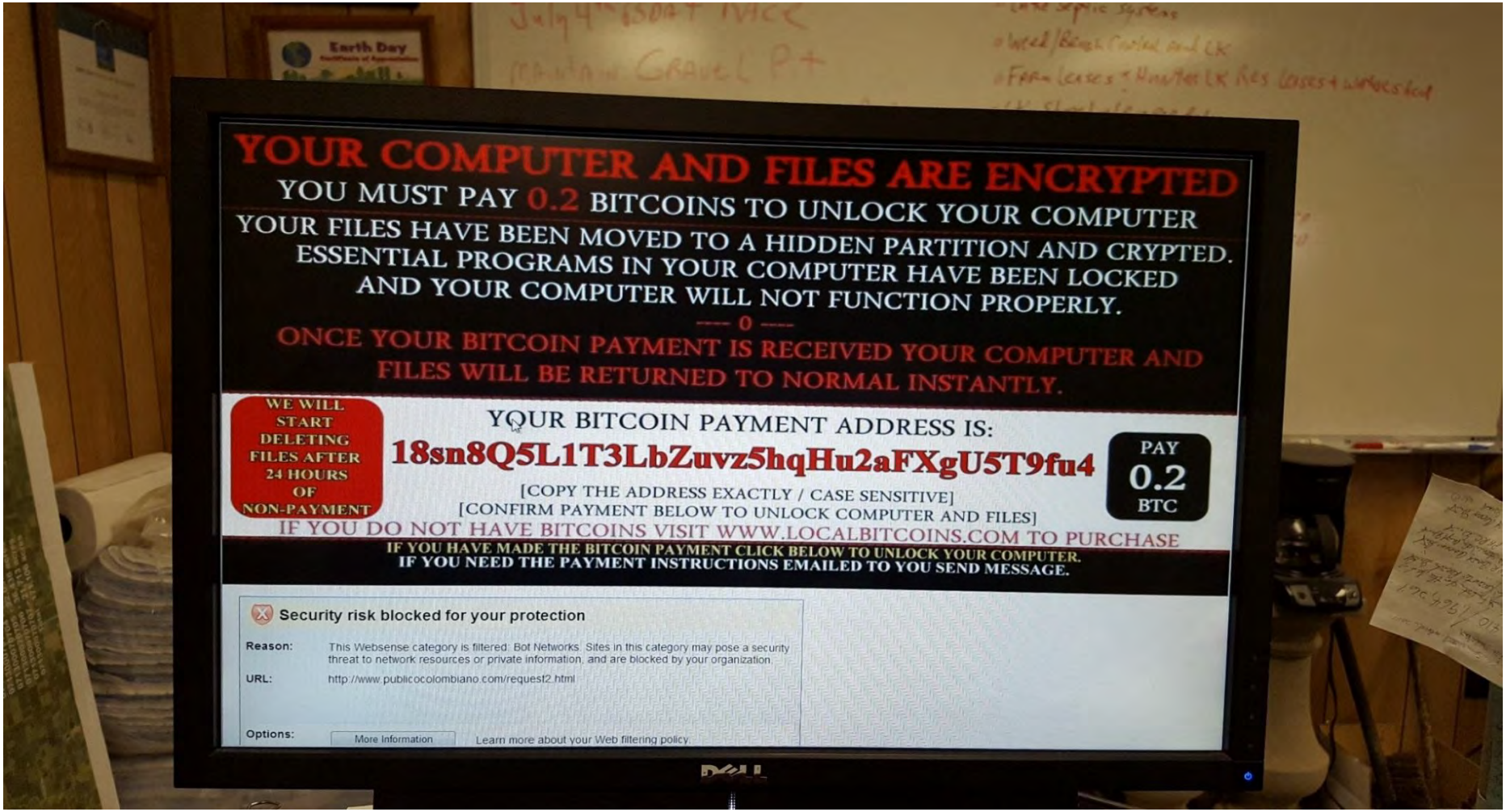


Electricity Threat Landscape



Man-made Threats

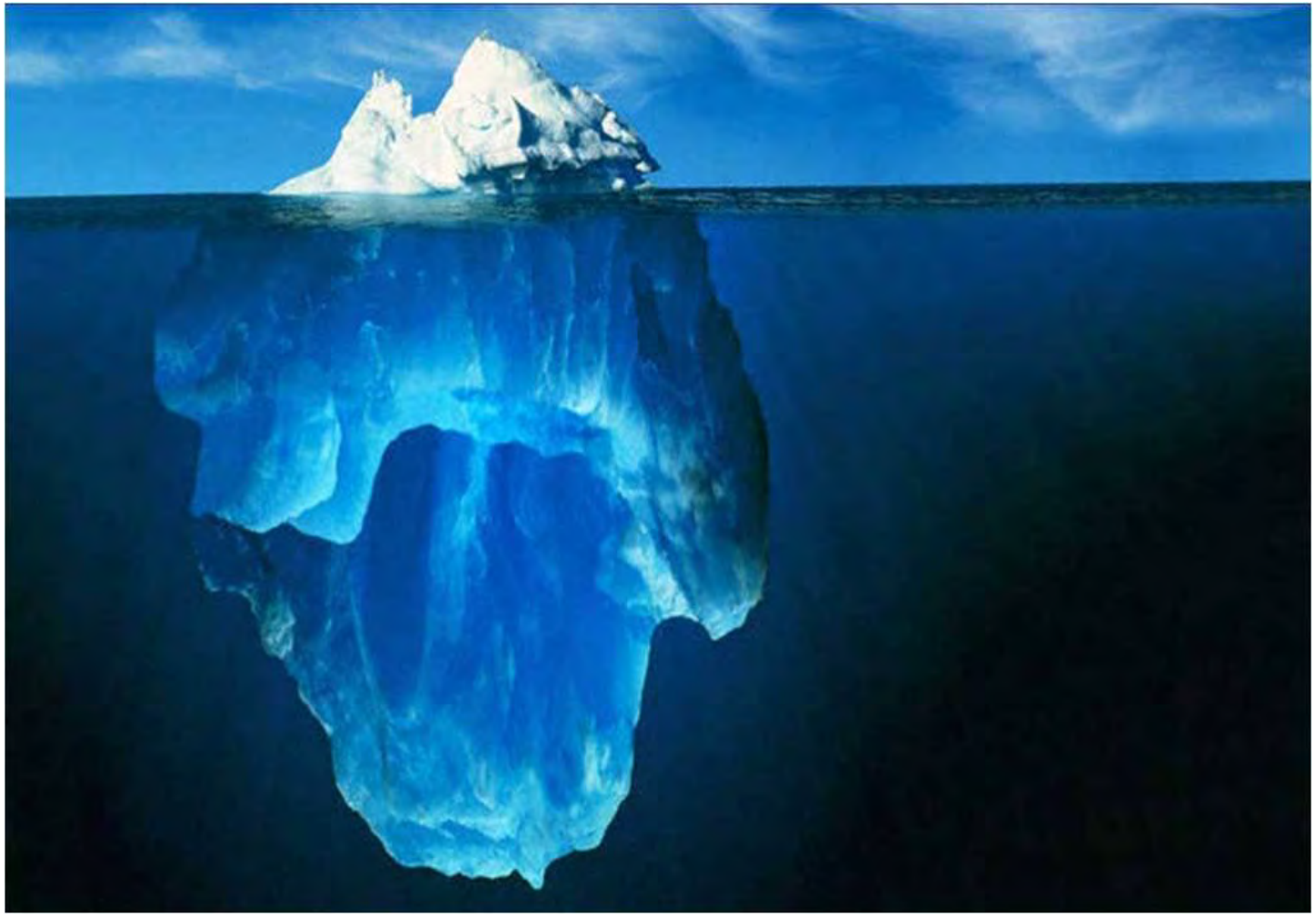
Ransomware


YOUR COMPUTER AND FILES ARE ENCRYPTED
YOU MUST PAY 0.2 BITCOINS TO UNLOCK YOUR COMPUTER
YOUR FILES HAVE BEEN MOVED TO A HIDDEN PARTITION AND CRYPTED.
ESSENTIAL PROGRAMS IN YOUR COMPUTER HAVE BEEN LOCKED
AND YOUR COMPUTER WILL NOT FUNCTION PROPERLY.
--- 0 ---
ONCE YOUR BITCOIN PAYMENT IS RECEIVED YOUR COMPUTER AND
FILES WILL BE RETURNED TO NORMAL INSTANTLY.
WE WILL START DELETING FILES AFTER 24 HOURS OF NON-PAYMENT
YOUR BITCOIN PAYMENT ADDRESS IS:
18sn8Q5L1T3LbZuvz5hqHu2aFXgU5T9fu4
PAY 0.2 BTC
[COPY THE ADDRESS EXACTLY / CASE SENSITIVE]
[CONFIRM PAYMENT BELOW TO UNLOCK COMPUTER AND FILES]
IF YOU DO NOT HAVE BITCOINS VISIT WWW.LOCALBITCOINS.COM TO PURCHASE
IF YOU HAVE MADE THE BITCOIN PAYMENT CLICK BELOW TO UNLOCK YOUR COMPUTER.
IF YOU NEED THE PAYMENT INSTRUCTIONS EMAILED TO YOU SEND MESSAGE.
Security risk blocked for your protection
Reason: This Websense category is filtered: Bot Networks. Sites in this category may pose a security threat to network resources or private information, and are blocked by your organization.
URL: http://www.publicocolombiano.com/request2.html
Options: More Information
Learn more about your Web filtering policy.

Security Challenges

- Cyber-attack vectors are multiplying:
  - System and network intrusions
  - Complex supply chain
  - Increased use of wireless communication and reliance on the internet
- Physical security
- Increased information sharing between public-private sector
- Security clearances
- Limited access to classified information
- Diverse regulatory oversight: federal, state, provincial

Tip of the Iceberg



Questions and Answers