Resiliency in the Electricity Subsector
Information Sharing and Exercises against Black Sky Events

Bill Lawrence, Director of Programs and Engagement
Cyber Resilient Energy Delivery Consortium
February 3, 2017
• Historical outages and NERC
• High Impact, Low Frequency (HILF) aka “Black Sky” events
• The Electricity Information Sharing and Analysis Center
• Recent threats and impacts
• GridEx
• **Quadrennial Energy Review (QER 1.2)**

![Diagram of Critical Infrastructure Interdependencies]

Key critical infrastructure interdependencies represent the core underlying framework that supports the American economy and society. The financial services sector (not pictured) is also a critical infrastructure with interdependencies across other major sectors supporting the U.S. economy.
High Impact, Low Frequency

- 1987 – NERC committee formed to address terrorism and sabotage
- 1999 – Electricity Sector Information Sharing and Analysis Center (ES-ISAC)
- 2004 – Critical Infrastructure Protection Committee (permanent)
- 2009/10 – HILF Report (joint DOE and NERC)
  - Pandemic Illness
  - Geomagnetic and Electromagnetic Events
  - Coordinated Cyber/Physical Attack
- 2011 – GridEx 2011
- 2012 – Severe Impact Resilience report
- 2012 – Cyber Attack report
- 2013 – GridEx II
- 2015 – GridEx III
EBOLA OUTBREAK
759 cases and 467 deaths since March

GUINEA
413 cases
303 deaths

SIERRA LEONE
239 cases
99 deaths

LIBERIA
107 cases
65 deaths

Image: CNN (4 July 2014)
Geomagnetic and Electromagnetic Events

Image: NASA

Image: Scientific American
• Stuxnet, Shamoon, Dragonfly/Energetic Bear, Havex/Black Energy
• Metcalf in California
Electricity Threat Landscape

- Squirrels
- Natural Disasters
- Physical Attack/Theft
- Cyber Attack
- Insider Threat/Catastrophic Human Error
- Coordinated Physical & Cyber Attack
- Supply Chain Disruption or Compromise
- Pandemics
- Geomagnetic Disturbance
- Direct Energy Weapon
- CBR Attack
- High-Altitude EMP
- Nuclear

Likelihood vs. Consequence

Resiliency | Reliability | Security
### Most Common Threat Agents

<table>
<thead>
<tr>
<th>Agent</th>
<th>Success</th>
</tr>
</thead>
<tbody>
<tr>
<td>Squirrel</td>
<td>879</td>
</tr>
<tr>
<td>Bird</td>
<td>434</td>
</tr>
<tr>
<td>Snake</td>
<td>83</td>
</tr>
<tr>
<td>Raccoon</td>
<td>72</td>
</tr>
<tr>
<td>Rat</td>
<td>36</td>
</tr>
<tr>
<td>Marten</td>
<td>22</td>
</tr>
<tr>
<td>Beaver</td>
<td>15</td>
</tr>
<tr>
<td>Jellyfish</td>
<td>13</td>
</tr>
<tr>
<td>Human</td>
<td>3*</td>
</tr>
</tbody>
</table>

CIP 014, Design Basis Threat document
Over 55,000 Substations over 100Kv
• ISAC concept introduced in Presidential Decision Document 63, published in 1998
  ▪ Electric power was identified as a critical sector along with 14 others
• Electricity sector’s ISAC has been hosted by NERC since 1999
  ▪ Recent concerns about sensitive information shared with the ISAC
  ▪ Could “leak” to NERC compliance and enforcement groups
  ▪ Caused a rethinking about the proper relationship
• ESCC identified strategic review of the ES-ISAC as a priority national security issue for 2015
  ▪ Strategic review initiated in January 2015, completed in June 2015
• ES-ISAC renamed to E-ISAC in September 2015
Mission

The E-ISAC reduces cyber and physical security risk to the electricity sector across North America by providing unique insights, leadership, and coordination.

Vision

To be a leading, trusted source for the analysis and sharing of Electricity Subsector security information.
Suspicious damage
Other damage
Criminal Threats - Copper Theft

POINT OF ENTRY

HEIGHT: 84'
Most Common Cyber Threat

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.

YOUR BITCOIN PAYMENT ADDRESS IS:

18sn8Q5L1T3LbZuvz5hqHu2aFXgU5T9fu4

PAY 0.2 BTC

[CONFIRM PAYMENT BELOW TO UNLOCK COMPUTER AND FILES]

WE WILL START DELETING FILES AFTER 24 HOURS OF NON-PAYMENT

[COPY THE ADDRESS EXACTLY / CASE SENSITIVE]

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 Website 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.publiccolonbano.com/requests2.html

Options: More Information  Learn more about your Web-filtering policy.
We encourage voluntary information sharing!

- **Cyber Security-related information sharing**
  - Indicators of compromise (such as IP addresses, domains, URLs, MD5s, etc.)
  - Forensics artifacts or samples (malicious email, malware, malicious binaries, logs or packet captures)
  - Reports (forensics, after action reports, or analysis)

- **Potential Operational Technology (OT) vulnerability issue sharing**
  - Unknown or unexplained PLC or RTU freezes, reboots, or failures
  - Discovered zero day vulnerabilities
We encourage voluntary information sharing!

- Physical Security-related Information Sharing
  - Breach/attempted intrusion of electricity facilities
  - Misrepresentation – presenting false information or misusing insignia, documents, and/or identification to misrepresent one’s affiliation as a means of concealing possible illegal activity
  - Theft/loss/diversion of key safety or security system, item, or technology
  - Sabotage/tampering/vandalism of facilities
  - Expressed or implied threats
  - Unusual observation or surveillance of facilities
• **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)
  - Cyber Risk Information Sharing Program (CRISP)
  - Physical security outreach visits

• **Tools**
  - E-ISAC portal (**www.eisac.com**)
  - Emergency notifications
  - STIX/TAXII automated information sharing
• Lately, we have seen opportunities to educate through events like E-ISAC/SANS Ukraine DUC – Defense Use Case
  ▪ Common threat and vulnerabilities and top twenty type controls
  ▪ Substantial opportunities in improved ways to view and manage OT environments

• Lessons learned from red team penetration tests
• NERC Level 2 Alert (two weeks prior)
• Internet of Things / DDoS White Paper
• CRISP and Data Repository, OT Pilot
• Cyber Automated Information Sharing System (CAISS) Pilot
• Portal Improvements / Platform Initiative
• Virtual Forensics (Malware Analysis Dropbox)
• DOE National Laboratory system
• DARPA RADICS
Scenario Time

GRID RELIABILITY LEVEL

Normal

Distributed Play

Nov 18
9 am – 1 pm

Nov 18
1 pm – 5 pm

Nov 19
9 am – 1 pm

Nov 19
1 pm – 5 pm

Move 1
T = 0 to 4 hours

Move 2
T = 4 to 8 hours

Move 3
T = 24 to 28 hours

Move 4
T = 72 to 76 hours

ESCC Calls

Executive Tabletop

Real time (Eastern)

Nov 19
11 am – 5 pm

ESCC Calls

Executive Tabletop

December +
The vision of the GridEx Program is to strengthen capability to respond to and recover from severe events:

- Exercising timely, real-world scenarios
- Increasing stakeholder participation and training value
- Increasing integration with BPS operations
- Greater state/provincial and local government participation
- Greater integration with U.S. and Canadian senior executives and government officials
- Including other most critically interdependent infrastructure sectors
- Increasing interactive simulation into joint simulation
Coordination with Government

NERC
Crisis Action Team

Electricity Subsector Coordinating Council (ESCC)

Regional Entities

Trade Associations

Energy GCC Other SCCs

Unified Coordination Group (UCG) or non-US equiv.

NERC Bulk Power System Awareness (BPSA)

E-ISAC
Electricity Information Sharing & Analysis Center

DOE
Department of Energy

DHS
NCCIC
ICS-CERT
US-CERT

Other Federal Agencies
US: FBI, FERC, DOD
Canada: Public Safety Canada, NRCan, RCMP, CSIS, CCIRC

NERC
Bulk Power System Awareness (BPSA)

Vendor Support
IT, ICS, ISP, Anti-virus

Other Critical Infrastructures
Telecommunications, Oil & Gas, others

ExCon - GridEx IV Exercise Control
NERC staff, GEWG, Booz Allen, Nat’l Labs, SMEs for Sim-cell, etc.

Executives Coordination

Electricity Subsector Coordinating Council (ESCC)

Coordinated Operations

Reliability Coordinators, Balancing Authorities, Generator Operators, Transmission Operators, Load Serving Entities, etc.

Local, State/Provincial Government

- Emergency Management Organizations
- Emergency Operations Centers / Fusion Centers
- Local FBI, PSAs, NG

Coordination with Government
• Exercise incident response plans
• Expand local and regional response
• Engage critical interdependencies
• Improve communication
• Gather lessons learned
• Engage senior leadership
Participation and Planning

E-ISAC
CIPC GEWG
Lead Planner
Planners
Players
Observers

Sub Teams

Planning
Physical
Cyber
Operations

Participants
Initial Scenario Discussion

GEWG scenario themes and potential attack vectors from GE3

Open Issues/Boundaries

- Watering hole/HAVEX
- USB in substation
- Shared tools/applications
- Comms links/MPLS
- Supply chain corruption
- Remote access infiltration
- Spearphishing
- Degradation of monitoring tools
- BCS issues

Cyber Attacks

- Distribution
- Simulated time of year
- Key personnel unavailability
- NERC/DOE as patient zero
- PMU/PDC
- GPS, EMP, GMD

Physical Attacks

- UAV threats
- Transmission line attack
- Leak of critical substations
- Scrubber damage
- Control center habitability
- Water intake degradation
- Fuel supply
- Active Shooter / explosives
- Vendor access to multiple sites
- Exfiltration of security plans
Continuing Coverage of the Power Grid Under Attack

SimDeckNewsSubmitted by on Thu, 11/19/2015 - 12:59
Organizations can voluntarily participate and set their level of involvement and internal level of effort.

Observing organization:
- Access to all planning/training materials and meetings, as well as the simulated social media tools.

Active organizations:
- Simplest
  - Partner with electric utilities (potentially with customers/providers) in local area and help with planning.
  - Exercise how electricity outages would impact your organization.
- More involved
  - Use the cyber/physical attack scenario materials to plan own-organization impacts with corresponding impacts to partner electricity utilities.
• Real world
• HILF – “what if?”
• Cyber / physical interdependencies
• Information sharing
• Exercising and customization

• Research leading to technologies and tools that improve the cyber-security of EDS OT
Questions and Answers

eisacevents@eisac.com