BASIN ELECTRIC
POWER COOPERATIVE

A Touchstone Energy® Cooperative

Basin Electric NERC CIP Program

2017 Minnesota Power Systems Conference

Mike Kraft

November 7, 2017

This presentation will discuss how to identify and implement cybersecurity best practices in a risk-based manner while maintaining CIP compliance. It will feature specific highlights and lessons learned.

BASIN ELECTRIC POWER COOPERATIVE
A Touchstone Energy® Cooperative

Introduction

Basin Electric Power Cooperative will provide cost-effective wholesale energy along with products and services that support and unite rural America.

BASIN ELECTRIC POWER COOPERATIVE
A Touchstone Energy® Cooperative

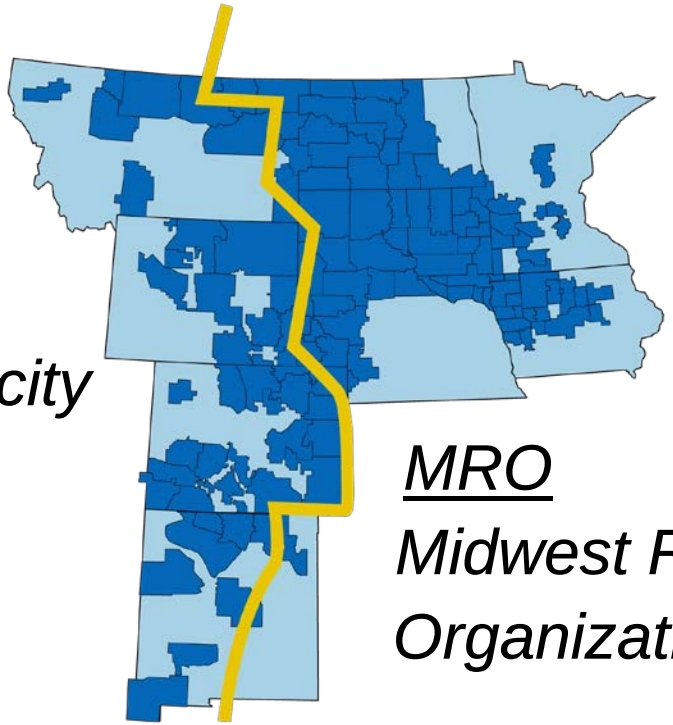
Profile

- A not-for-profit generation and transmission cooperative incorporated in 1961 to provide supplemental power to a consortium of rural electric cooperatives
- Diverse energy portfolio: coal, gas, oil, nuclear, distributed, and renewable energy
- Consumer owned by 141 member cooperative systems
- Members' service territories comprise 540,000 square miles in nine states
- Operates >5,200 megawatts (MW) of wholesale electric generating capacity
- Owns 2,356 miles and maintains 2,441 miles of high-voltage transmission, and owns and maintains equipment in 81 switchyards and 195 telecommunication sites
- Serves 3 million electric consumers

BASIN ELECTRIC POWER COOPERATIVE
A Touchstone Energy® Cooperative

Service Area

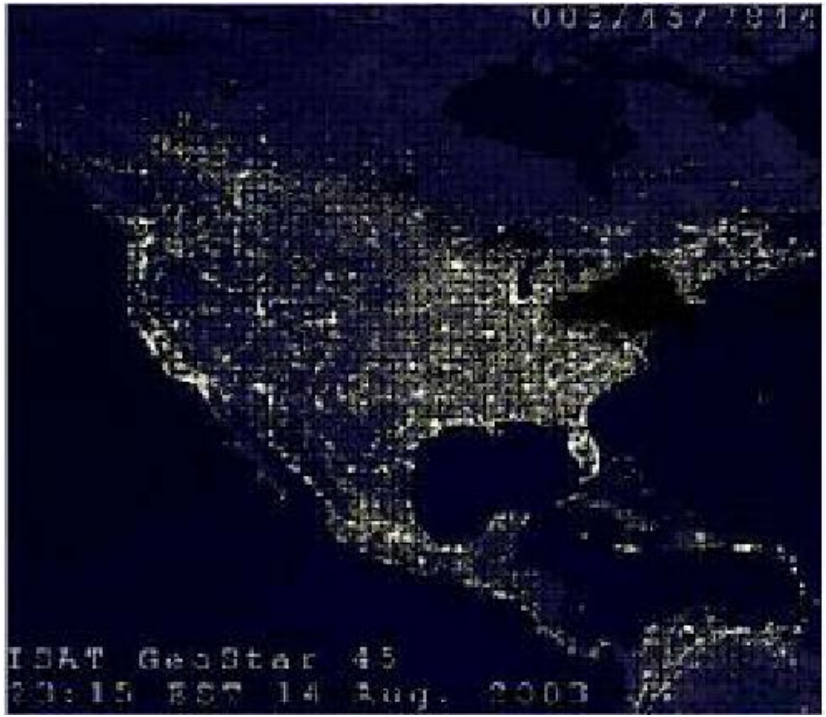
<u>WECC</u>
Western Electricity Coordinating Council



<u>MRO</u>
Midwest Reliability Organization

BASIN ELECTRIC POWER COOPERATIVE
A Touchstone Energy® Cooperative

In the beginning…



BASIN ELECTRIC POWER COOPERATIVE
A Touchstone Energy® Cooperative

Warnings

- Hacktivist, Ecoterrorist, Criminal, Espionage, Terrorism, State sponsored/Disruptive
- Shamoon, Stuxnet, Duqu, Flame, Havex, Blackenergy, Crashoverride
- Ransomware, Phishing, Malware
- Metcalfe, Ukraine, Ukraine part 2

“The threat landscape is constantly changing and requires adaptation and information sharing on how best to address these issues in an effective and efficient manner.” -NERC report to FERC

BASIN ELECTRIC POWER COOPERATIVE
A Touchstone Energy® Cooperative

Buzzing

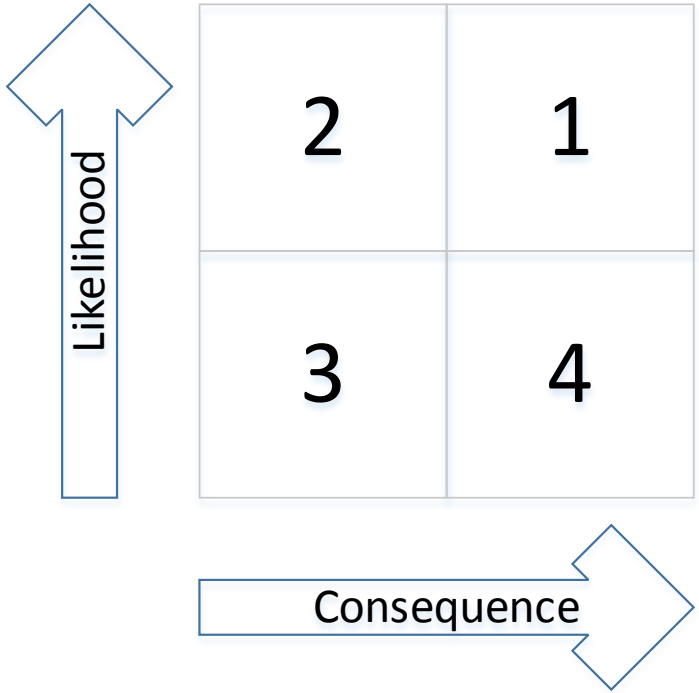
- It’s going to take a 9/11 in the cyber realm
- The next Pearl Harbor will be cyber
- Cybersecurity Poverty Line
- Patch or Perish
- Skate to where the puck will be
- Plans are useless, but planning is indispensable
- Tools in the toolbox
- Arrows in the quiver
- Bring a wrench to a gun fight

Risk

- Operational
- Financial
- Reputational
- Compliance
- Existential

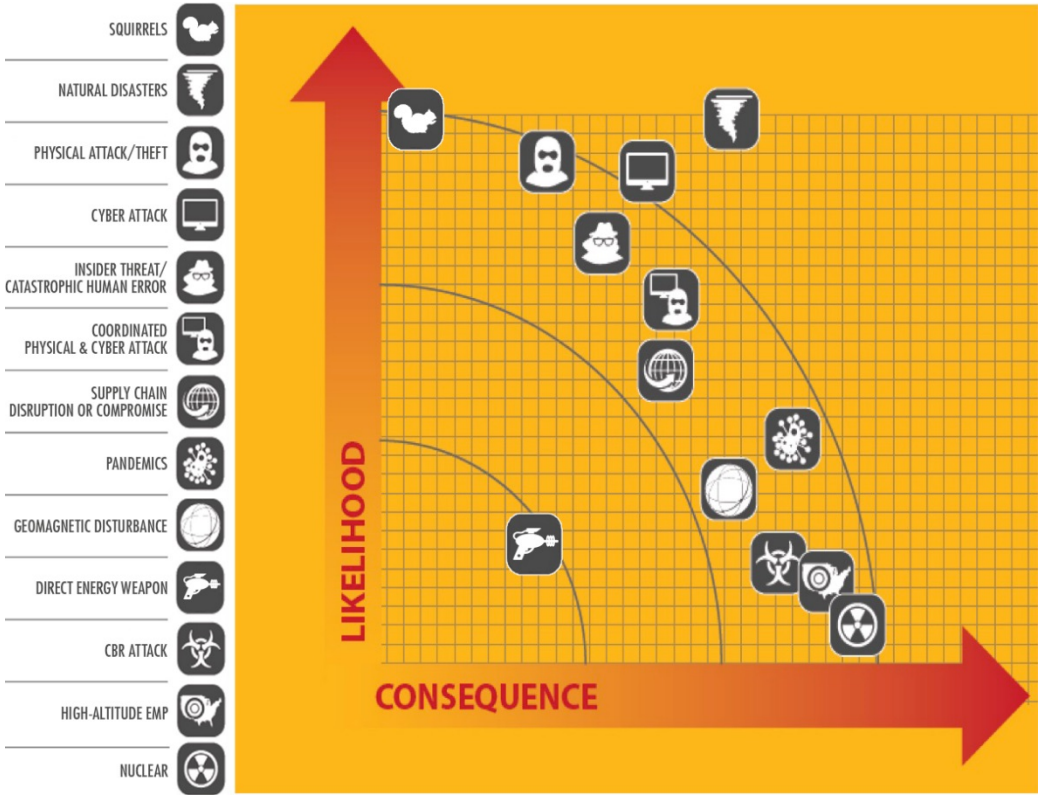
BASIN ELECTRIC POWER COOPERATIVE
A Touchstone Energy® Cooperative

Threat Matrix



BASIN ELECTRIC POWER COOPERATIVE
A Touchstone Energy® Cooperative

Threat Matrix



BASIN ELECTRIC POWER COOPERATIVE
A Touchstone Energy® Cooperative

What is Critical Infrastructure Protection (CIP)

The NERC Critical Infrastructure Protection (CIP) standards provide requirements to protect the bulk power system from cyber and physical attacks on critical infrastructure. The CIP standards require users, owners, and operators of the bulk power system to identify and categorize cyber systems based on “bright-line” criteria for the application of cyber security requirements commensurate with the adverse impact that loss, compromise, or misuse of those cyber systems could have on the reliable operation of the interconnected transmission network. Once these assets are identified, the CIP standards require that the responsible entities establish plans, protocols, and controls to safeguard physical and electronic access to these systems, train personnel on security matters, report security incidents, and be prepared for recovery actions.

Source: FERC Reliability Primer

https://www.ferc.gov/legal/staff-reports/2016/reliability-primer.pdf

Compliance <> Security

BASIN ELECTRIC
POWER COOPERATIVE
A Touchstone Energy® Cooperative

Critical Infrastructure Protection Philosophy

"Identify and implement cyber security best practices in a risk based manner while maintaining CIP compliance."

-NERC Executive Oversight Committee, 12/15/2014

BASIN ELECTRIC POWER COOPERATIVE
A Touchstone Energy® Cooperative

Critical Infrastructure Protection (CIP) Response

- NERC CIP Regulation (CIP-002 through CIP-011 and CIP-014)
- Tone from the Top
- Internal Compliance Program
- Responsibility and Accountability
- Resources - People and investments
- Policies / Programs / Plans / Procedures
- Assets / Facilities / Elements
- Business Practices

BASIN ELECTRIC POWER COOPERATIVE
A Touchstone Energy® Cooperative

Critical Infrastructure Protection (CIP) Response

- CIP Senior Manager
- CIP Program Manager
- CIP Project Managers
- CIP Designated Positions
- CIP Subject Matter Experts (SMEs)
- Programs
- Facilities
- Controls
- Investments

BASIN ELECTRIC POWER COOPERATIVE
A Touchstone Energy® Cooperative

Best Practices

- Relationships are key - Plug in
- Security Clearances
- Threat Intelligence - classified and open source
- Frameworks - NIST & CIP
- Procurement Practices/Supply Chain
- Insider Threat
- Cyber Mutual Assistance (CMA)
- Exercises (e.g. GridEx)
- Know thyself
- Defend thyself

BASIN ELECTRIC POWER COOPERATIVE
A Touchstone Energy® Cooperative

Relationships

- E-ISAC (Electricity-Information Sharing and Analysis Center)
- Public-Private partnerships: Federal, State, Local
- Government: DOE, DHS, FBI, Fusion Centers
- Industry: NATF, NAGF, NRECA, EEI, APPA, ESCC
- Regions: MRO, WECC
- Compliance Forums: MCCF, WICF
- Cross sector coordination (e.g. Communications, Natural Gas, Water, Banking and Finance)
- Vendors
- Open source

BASIN ELECTRIC POWER COOPERATIVE
A Touchstone Energy® Cooperative

NCCIC Seven Strategies

- Implement application whitelisting
- Ensure proper configuration/patch management
- Reduce your attack surface area
- Build a defendable environment
- Manage authentication
- Implement secure remote access
- Monitor and respond

Source: National Cybersecurity and Communications Integration Center

https://ics-cert.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf

BASIN ELECTRIC POWER COOPERATIVE
A Touchstone Energy® Cooperative

Lessons Learned

- Time - what starts the clock
- How do you track
- Managing information
- Procedures for BCSs, BCAs, EACMS, PACS, etc…
- Evidence to demonstrate compliance
- “Best practices”
- Resiliency vs. Prevention

BASIN ELECTRIC POWER COOPERATIVE
A Touchstone Energy® Cooperative

More Lessons Learned

- ADKAR - Awareness, Desire, Knowledge, Ability, Reinforcement
- Culture - Like Safety but Electric Reliability
- CIP moving target -> steady state
- Ownership
- Right people change over time - SME identification/changes
- Relationships are key component
- Resources
- Terminology
- Operationalizing - Consistent & Repeatable processes

Thoughts

- Risk informed: Common understanding of risk
- Risk Mitigation: No silver bullet, nor guarantees
- Correct people talking about correct systems
- Redundancy and Resiliency are necessary
- Relationships are key
- Working on maturation of security culture
- Cyber Threat is growing and evolving

BASIN ELECTRIC POWER COOPERATIVE
A Touchstone Energy® Cooperative

Questions

Mike Kraft
Critical Infrastructure Protection (CIP) Program Manager
Basin Electric Power Cooperative
1717 E Interstate Avenue
Bismarck, ND 58503
Direct: 701-557-5522
mkraft@bepc.com
http://www.basinelectric.com/

BASIN ELECTRIC POWER COOPERATIVE
A Touchstone Energy® Cooperative