Risk Analysis & Management for Cybersecurity

July 11, 2017

Missouri PSC Cybersecurity Workshop

Sharon Thomas

Senior Manager, Research Lab, NARUC

Overview

- What methodologies are being used for risk management and analysis?

- How might current methodologies be improved?

- How can mutual aid play a role in risk management?

Methodologies for Performing Risk Analysis and Risk Management

- NIST Cybersecurity Framework

- DOE Electricity Subsector Capability Maturity Model (ES-C2M2)

- DOE Electricity Sector Cybersecurity Risk Management Process (RMP) Guideline

- Bayesian Probability

How Can We Improve These Methodologies?

- NIST CSF:
  - Creation of a web-based knowledge center with resources in one place

- ES-C2M2 & RMP:
  - Geared towards practitioners; abstract
  - ES-C2M2 evaluates implementation; helps with cost recovery but not prudency
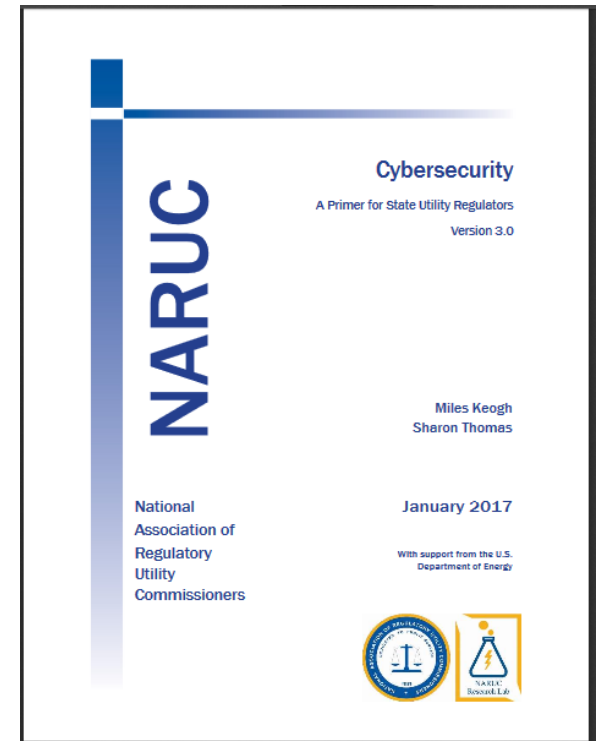
How Can We Improve These Methodologies?

- NARUC's Cyber Risk Management Tool for Regulators

  Part I: Strategy Development

  Guidance

  Part II: NARUC's Cyber Primer 3.0

  Questions

  Part III: Bayesian Cyber Evaluative

  Tool

Cybersecurity

A Primer for State Utility Regulators

Version 3.0

NARUC

Miles Keogh
Sharon Thomas

National
Association of
Regulatory
Utility
Commissioners

January 2017

With support from the U.S.
Department of Energy

Link to Primer: http://bit.ly/CyberPrimer

Can a Mutual Aid Paradigm Assist in Risk Management?

Thank You!

Sharon Thomas

Senior Manager, Research Lab, NARUC

202-384-1572; sthomas@naruc.org