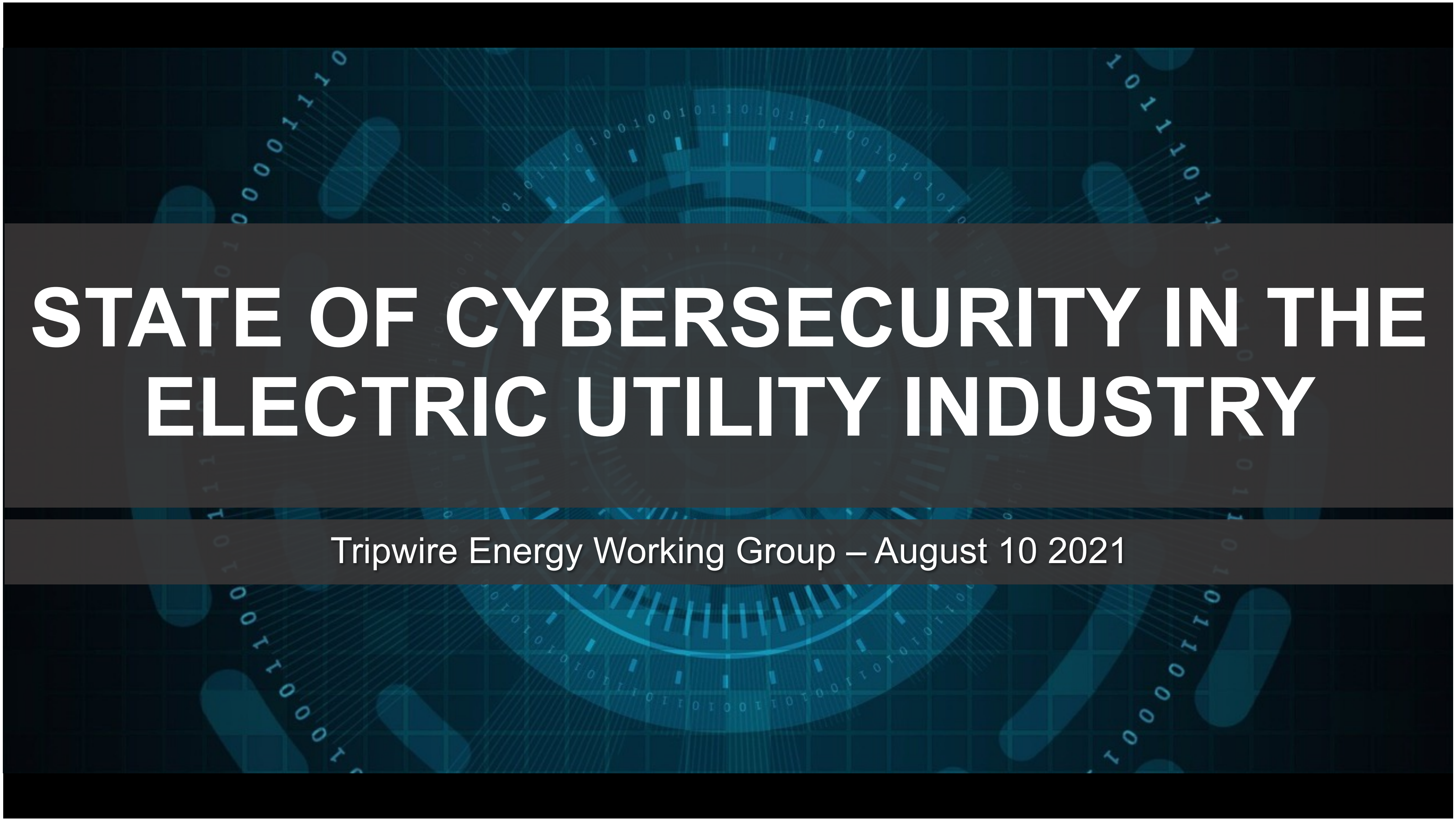

STATE OF CYBERSECURITY IN THE ELECTRIC UTILITY INDUSTRY

Tripwire Energy Working Group – August 10 2021

INTRODUCTION

- Former utility staff (telecommunications, water & electric)
- First NERC CIP auditor in the US
- Drafter of NERC CIP standards and formal interpretations
- NERC CIP Supply Chain Working Group contributor
- Former Principal Investigator US DOE National Electric Sector Cybersecurity Organization
- EnergySec Founder, Director and President Emeritus
- Centro de Ciberseguridad Industrial (CCI) US Coordinator
- Cybersecurity Advisory Team for State Solar, NARUC/NASEO
- Advisor to multiple industrial security product vendors
- GCIP, CISA, CRISC, CISSP-ISSAP, SSCP, NSA-IAM, CVI, TCP, SCP

GLOBAL SITUATION

- Infrastructure is a target
- Your adversaries have three things you don’t
- Who are you up against?
  - Organized crime
  - Nation states
  - Non-governmental organizations (NGOs)
  - Competitors
  - Ourselves (Hanlon’s Razor)
- We all buy our gear from the same sources
- Attribution is getting better
- Cyber warfare, espionage and prosecution norms

CRYSTAL BALL

- Each “catalytic event” creates a cyber-avalanche
- NERC CIP moved the needle for electric sector, everyone noticed
- Legislators, regulators and commissions are getting wiser
  - 18 new cybersecurity bills introduced in just this session
- Regulation to the rescue!
- Real world examples:
  - Global trend (NIS, CAF, BSI, 62443, NIST 800-53/82/CSF, NERC CIP)
  - FERC RFI seeking to align with NIST
  - 100-day Plan to Address Cybersecurity Risks
  - ES-C2M2 (new version) & ONG C2-M2 being used by commissions and underwriters
  - TSA Pipeline Security Guidelines updated, Security Directives (x2); API 1164
  - DHS CISA ICS attack history
  - Recent updates to CFATS
  - Too many Executive Orders to list
  - New National Security Memorandum

NATIONAL SECURITY MEMORANDUM

- Not a law/regulation – voluntary collaborative initiative (for now)
- Baseline security controls across all critical infra sectors
- Some controls will be common with existing frameworks (CIP)
- NIST 800-53/82 are being promoted (expected) to be the set
- Measurement (no enforcement) will be DHS CISA and SSA
- Unclear how measurement will happen (audit, assessment?)
- Will apply first to electricity subsector, then gas, chemical, water
  - Unclear if "National Security" banner will loop in Distribution
- Final framework to be completed by July 28, 2022
- Clear signaling that participation is expected, or else…

NSM – WHAT DO I NEED TO DO?

- “…deployment of technologies and systems that provide threat [and anomaly] visibility, indications, detection, and warnings…”

- “…response capabilities for cybersecurity in essential control system and operational technology networks…”

- …” Government and industry to collaborate to take immediate action…”

- “…baseline cybersecurity goals that are consistent across all critical infrastructure sectors…”

NSM – RECOMMENDED ACTIONS

- Gap assessment of current CIP controls against 800-53/82
  - CIP has already been mapped, use existing tools
- Create action plan to remediate any control gaps
  - Owners, actions, dates, budget
- Begin any architecture/system modifications needed for increased monitoring, detection, response and recovery
- Procure and/or tune network anomaly detection software
  - CRISP, Neighborhood Keeper, Essence or other
- Establish trained and resourced security operations function
  - Can be outsourced or insourced
  - Process, analyze, respond and tune new tools
- Perform REAL incident and recovery response exercises

NSA – VOLUNTARY VS. MANDATORY

- PR incentives/hit – public perception minimum bar has been set
- Cyber insurance impacts can be very real
- Business partnerships – upstream/downstream; M&A, contracts
- Constrained markets over time
- Earlier adopter bonus points with oversight body
- Easier to demonstrate proactive continuous improvement vs. late-stage, time-constrained, forced, and reactive efforts
- Given the situational gravity, it may be inevitable
- If not the NSM, then any one of the other “influences”

DIRECT SIGNALING

"...defend US critical infrastructure by encouraging & facilitating deployment of tech & systems that provide threat visibility, indications, detection, & warnings, & that facilitate response capabilities for cybersecurity in essential control system & operational tech networks.”

"We’re committed to addressing it. We’re starting with voluntary, as much as we can, because we want to do this in full partnership. And — but we’re also pursuing all options we have in order to make the rapid progress we need.”

"...multiple administrations have recognized that there are no mandated authorities to mandate cybersecurity requirements for critical infrastructure... in the context of our openly saying that we really are committed to addressing the limited and piecemeal regulation...”

"The President is essentially saying, 'We expect responsible owners and operators to meet these performance goals. We will look to you to implement this.’”

- National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems, The White House

June 28, 2021

COMMON SOLUTION THREADS

- For organizations already subject to NERC CIP, much can be borrowed
- Other controls frameworks also exist for an “overlay” (mapping) approach to managing compliance risk
- Portable skill sets across sector types in OT
  - IT already has common skill pool
- Some Common solutions exist for IT and OT
  - Hardware
  - Software

“REGULATORY” FORECAST

- Whether direct regulation (CIP, TSA, AWWA, CFATS) or indirect “transitive” regulation (NIST, EO, NSM), new normal is:
  - Buy only “trusted” hardware, software, services
  - Know all cyber assets in your environment
  - Know the security posture for all cyber assets
  - Segment and restrict access (zero trust, MFA)
  - Monitoring and detection at asset and network level
  - Strong incident response capability
  - Strong recovery capability
- Less “guessing” - aligns with guidelines, regulation, Executive Orders, National Security Memos, etc. in peer sectors
- Get ahead of this before it is mandated

ASSETS AND ARCHITECTURE

- Do you have an asset inventory?
  - Not everything, but even just the critical stuff
  - Back it with change control or expect drift (waste time/money)
- Do you have an environment you can defend?
  - Segmented networks
  - One-way traffic
  - MFA and strict remote access controls
  - Shear-away networks, “crumple zones,” intelligent islanding
- Interdependencies can be your Achilles heel
  - Runs converse to many current approaches

IN THE LAND OF THE BLIND

- Would you know – with sufficient confidence – if there was (or was not) an adversary in your system?
- Monitoring is in every federal conversation now
  - CRISP, Neighborhood Keeper, Essense…
- “Smoke detectors” will be required in the “building code”
- Regulation, insurance, diligence, reporting (data breach)
- Start where you can, tune, then lather, rinse, repeat
- Based on solid asset inventory and feeds response and/or recovery

SUPPLY CHAIN RISK MANAGEMENT

- NERC CIP-013 is the tip of the iceberg
  - Adding new asset types and moving to low impact
- Multiple Executive Orders, probably more to come
- ”No-buy” lists, rip/replace, legacy risk often unaddressed
- “Made in” often means “assembled in”
- How far do you go? Was it far enough?
- HBOM, SBOM, FBOM
- CyberStar, transparency centers, certification, validation
- Frustration and costs go up for everyone

PRACTICE LIKE IT’S GAME DAY

- When was the last time you did a **real** incident response exercise?
  - Did it include a recovery drill?
  - Did it include IT impacting OT through business process?
- Everything else leads up to this
  - Asset inventory, supply chain, segmentation, monitoring
- Borrow from operations (and safety)
  - Can you really go to manual? For how long?
- Expect “oversight” and media when it happens
  - Cyber NTSB, CISA, E-ISAC, FBI, Commerce, State…
- What happens to one utility will affect all others…

NERC CIP HORIZON

- Legislators, regulators and agencies are getting wiser
- Drifting toward NIST (FERC RFI)
- Focus on CIP-007, CIP-008 and CIP-009
  - Monitoring, incident response, and recovery
- Supply Chain
  - Coming to a Low Impact asset near you
- Cloud (BCSI and BCS)
- Virtualization
  - Biggest shift in CIP since v3 to v5
- Global adoption is picking up steam

NON-REGULATORY FORECAST

- Innovation is accelerating disruption and disruption
- OT looking more like IT, getting closer to just T
- Smart everything will be connected to smart everything
- Ever increasing dependence on technology and data
- Losing touch with manual options
- Artificially intelligent systems can still be hacked
- Competing forces of unregulated greenfield business in distribution vs. threat of regulation for distribution

DATA WILL ALSO BE YOUR BUSINESS

- Digital transformation, convergence & other buzzwords
- Data is the new oil …and also the new toxic waste
- Everything you buy is digital now, with a connection
- What happens when everything in your operation generates a data (revenue) stream?
- Someone else can do it faster and better than you
- You may possibly make more revenue from operational data than the electrons used to create the data

EMBRACING THE FUTURE

- More regulation is coming – must be “this tall” to ride
  - Will likely go beyond NERC CIP, but not by much
  - Wider possible applicability
- Regulations and standards will shift with threats and tech
  - For example, ransomware…
- Control norms are emerging for both OT and IT, globally
- Technology is transforming how we can do business
  - Data as a revenue stream will become more common
- Regulation is changing to allow new virtualized and cloud models for data, applications and even infrastructure
  - GoToMySCADA/HMI/DCS/EMS/PLC/DigitalTwin is a thing

CONTACT ME

@PATRICKCMILLER

LINKEDIN.COM/IN/MILLERPATRICKC

PMILLER@AMPERESEC.COM

WWW.AMPERESEC.COM

+1.503.272.1414