The 3rd Next Generation Cyber Security for Utilities Conference
February 13-14, 2019 • Denver, CO

SITE TOUR • TRI-STATE GENERATION & TRANSMISSION • TUESDAY, FEBRUARY 12, 2019

1:00 PM	DEPARTURE FROM VENUE
1:25 PM	ARRIVAL AT TRI-STATE GENERATION AND TRANSMISSION / GREETING BY STAFF / REGISTRATION WITH SECURITY
1:35 PM	TOUR OF ENERGY MARKET
2:00 PM	TOUR OF TRANSMISSION DISPATCH
2:30 PM	REFRESHMENTS / OUTSTANDING QUESTIONS
2:45 PM	DEPARTURE FROM TRI-STATE GENERATION AND TRANSMISSION

Westminster, Colorado-based Tri-State Generation and Transmission Association is a not-for-profit, cooperative wholesale power supplier to 43 member electric distribution cooperatives and public power districts that collectively serve more than one million consumers across Colorado, Nebraska, New Mexico and Wyoming. The association's more than 1,500 employees focus on delivering members reliable and affordable power and a wide range of services. Created by its members in 1952, today Tri-State delivers electricity generated from coal, natural gas and renewable energy across a 5,562-mile high-voltage transmission system.

CONFERENCE DAY ONE • WEDNESDAY, FEBRUARY 13, 2019

8:00 AM — REGISTRATION AND COFFEE

9:00 AM — CHAIRPERSON'S OPENING REMARKS

9:15 AM — CONFERENCE PRESENTATION: OUTLOOK FOR THE FUTURE OF CYBER SECURITY'S ROLE IN UTILITIES

- Emphasizing the growing necessity for cyber security programs through trend analysis and case studies
- Projecting likely sources of future attacks and their severity in the current and projected geopolitical and projected geopolitical climate
- Identifying, at a high level, the "how's" of several known attacks and the impact they've had against their targets

10:00 AM — CONFERENCE PRESENTATION: UPDATED REPORTING STANDARDS AND EFFECTIVE SHARING OF INCIDENT DATA

- Spreading awareness of possible future incursion tecniques through adequate reporting of disrupted reliability tasks
- Increasing quality of reporting by establishing nationwide standards to minimize information loss due to data interpretation disparities
- Avoiding understating, or overstating, modern threats by analyzing mass amounts of incident data and drawing conclusions
- Speeding up initial incident awareness by forming inter-organizational agreements

Simon Slobodnik, IT Specialist
FEDERAL ENERGY REGULATORY COMMISSION

10:45 AM — MORNING REFRESHMENTS

11:15 AM — SESSION ONE: TALENT ACQUISITION AND TEAM DEVELOPMENT STRATEGIES

- Accessing new talent pools by establishing recruiting programs targeting recent college graduates
- Forming an effective training program to bring new recruits up to speed and standardize their skill set
- Outlining legal implications of an attack outcome to incentivize executive staff to allot a greater budget to maintaining an adequate team size

Charles Salas, Manager of Industrial Cyber Security
EXELON

The 3rd Next Generation Cyber Security for Utilities Conference
February 13-14, 2019 • Denver, CO

12:30 PM — **LUNCH**

1:30 PM — **CONFERENCE PRESENTATION: Cyber Mutual Assistance – A New Model for Electric Companies Preparing and Responding to Cyber Security Emergencies**

- Today, the electric industry's culture of mutual assistance is a model for creating responses to cyber threats to the energy grid
- It is a natural extension of the electric power industry's longstanding approach of sharing critical personnel and equipment when responding to emergencies
- The Cyber Mutual Assistance Program was developed based on lessons learned from major destructive cyber incidents overseas and from exercises in North America
- This presentation will describe what it is and how it addresses risks faced by critical infrastructure owners and operators

Kaitlin Brennan, Manager of Cyber & Infrastructure Security
Edison Electric Institute

2:15 PM — **SESSION TWO: The Growing Activity of State-Sponsored Threat Actors**

- Determining the source and frequency of probing efforts to draw conclusions towards the intent and scale of future attacks
- Leveraging federally determined assets and penalizations against foreign agents to deliver a response to malfeasance
- Detailing the characteristics of Industroyer and other forms of malware used by state-sponsored hackers

Glen Chason, Senior Consultant of Industrial Control Systems
Mandiant

3:30 PM — **AFTERNOON REFRESHMENTS**

4:00 PM — **PANEL DISCUSSION: Metrics and Measurement of Security System Quality**

- Noting the pitfalls associated with using budget or staff size to quantify security capabilities
- Utilizing peer comparing data to contrast response trends with similar security teams and help establish standards
- Designing security controls to be in compliance with policy, process or procedure

Andrew Bochman, Senior Cyber & Energy Security Strategist
Idaho National Laboratory

Ryan Spelman, Senior Director of Business Development
Center for Internet Security

4:45 PM — **CONFERENCE PRESENTATION: Steps to Achieve a Total Integration of IT/OT Systems**

- Augmenting OT protection from anomalies by achieving real-time visibility through convergence
- Bridging the knowledge gap between IT and OT through senior leadership and collaborative culture
- Curtailing monitoring complexities by reducing the amount of devices being watched at any given time through IT implementation

5:30 PM — **CLOSE OF DAY ONE**

CONFERENCE DAY TWO • THURSDAY, FEBRUARY 14, 2019

8:30 AM — **REGISTRATION AND COFFEE**

9:00 AM — **CHAIRPERSON'S OPENING REMARKS**

9:05 AM — **CONFERENCE PRESENTATION: ISOC Implementation and Methodology**

- Coordinating surveillance perspectives to eliminate blind spots and create a more comprehensive infrastructure
- Employing threat indicators and intelligence-driven defense to improve overall response times
- Constructing an information silo to monitor systems in real-time, establishing a new norm for leveraging data analytics

Ralph King, Cyber Security Program Manager
Electric Power Research Institute

The 3rd Next Generation Cyber Security for Utilities Conference
February 13-14, 2019 • Denver, CO

9:50 AM

CONFERENCE PRESENTATION: ADDRESSING CYBERSECURITY RISK IN YOUR SUPPLY CHAIN

- Minimizing risks by engaging and sharing information with trusted vendors and outside entities
- Carefully monitoring connections between critical machines and outside networks
- Educating users on identifying threat vectors and taking protective measures to play their part in keeping the company secure

Brian Gatus, Principal Manager of Indirect Procurement
SOUTHERN CALIFORNIA EDISON

10:35 AM

MORNING REFRESHMENTS

11:05 AM

PANEL DISCUSSION: THREAT VECTOR ANALYSIS AND SECURITY DILIGENCE

- Being mindful of the broader access to systems resulting from increasing connectivity associated with IoT devices
- Keeping track of new vulnerabilities to your ICS that result from new additions or integration
- Promoting greater security requirements for the exchange and collection of sensitive data by being conscious of network paths created by new customers

Reid Fudge, CISO/Enterprise Risk Management
TRI-STATE GENERATION AND TRANSMISSION ASSOCIATION, INC.

11:50 PM

CONFERENCE PRESENTATION: BLOCKCHAIN AND ITS POTENTIAL TO DRAMATICALLY SHIFT UTILITY APPROACHES TO SYSTEM STRUCTURING

- Managing sales, payments and distribution in a more accountable fashion by getting away from a centralized information flow
- Dodging possible inaccuracies and discrepancies by using smart contracts to record incoming data to a blockchain ledger
- Heightening response times by catching anomalies in real-time with automated checking of information nodes

12:35 PM

LUNCH

1:35 PM

CONFERENCE PRESENTATION: BUILDING TEAM CONFIDENCE AND RESPONSE EFFECTIVENESS THROUGH CONDUCTING AND DEVELOPING DRILLS

- Tailoring exercises to keep up-to-date with known agent capabilities, such as their ability to “throw switches”
- Raising drill effectiveness by periodic tweaking of scenarios to promote creative problem solving and malleability
- Composing situations reflective of blackstart to prepare teams for catastrophic circumstances

Andrew Bochman, Senior Cyber & Energy Security Strategist
IDAHO NATIONAL LABORATORY

2:20 PM

SESSION THREE: ARTIFICIAL INTELLIGENCE’S PROFICIENCY IN THREAT MITIGATION

- Locating active malware in a system by using AI to identify it by function or precursor operations, rather than location
- Investigating the source of infiltration through discerning missing information and drawing logical conclusions
- Augmenting human efforts to prevent cyber-attacks by adding another dimension to efforts to combat ever-evolving threats

3:35 PM

CHAIRPERSON’S CLOSING REMARKS

3:45 PM

END OF CONFERENCE AND AFTERNOON REFRESHMENTS