Utility Cyber Security Forum

December 11, 2019 • Chicago

Program Schedule

Tuesday, December 10, 2019

5.00 – 6.00 **Pre-Conference Drink Reception for All Conference Participants**

6.00 – 8.00 **Networking Dinner for All Conference Participants**
Location: Prime & Provision Steakhouse, 222 N LaSalle St, Chicago

Wednesday, December 11, 2019

8.00 – 9.00 **Registration and Continental Breakfast**

9.00 -9.30 **Industrial Cyber Security: A Utility Perspective From the Trenches**

Charles Salas, Manager – Industrial Cyber Security, Exelon

9.30 -10.00 **Best Practices in Utility Cybersecurity Project**

ProtectOurPower.org is a family-funded non-for-profit interested in a more reliable and resilient grid. Given that Mission, the organization pursues a number of projects in that vein. One of those projects is focused on surfacing best practices (as an enhancement to NERC CIP Compliance) for utility practitioners. Paul will describe this project and review the current status.

Paul Feldman, Past Chairman, Midcontinent ISO (MISO); Former Board Director, Western Electricity Coordinating Council (WECC)

Mr. Feldman is past Chairman of the Midcontinent ISO (MISO) and a former Board Director of the Western Electricity Coordinating Council (WECC). He was CEO of Columbia Energy, CEO of Utilicorp United, and SVP of AES. Presently, Mr. Feldman serves as a Board member at Blattner Energy, Opus One, Indeco, and EnergySec. He has been appointed to serve on the NCC and advise the Secretary of Energy on matters related to electricity and transmission systems. He also serves as a member of the National Renewable Energy Laboratory in Golden on the Energy Systems Integration Technical Review Panel. He serves as Senior Advisor to Protect Our Power, Exacter Inc., and Claroty.

10.00-10.30 **Best Practices to Review CIP Firewall Rulesets**

The growing complexity of today's network infrastructure makes the task of configuring firewalls for security and compliance increasingly challenging. The objective of this presentation is to learn how to leverage technology such as NP-View to quickly identify configuration issues and to automate the ruleset review process. The presentation will cover setting a firewall ruleset review workflow, network map visualization, and access policy verification to prepare clear CIP compliance reports.

Dr Robin Berthier, Co-Founder and CEO, Network Perception

Robin has over 15 years of experience in the design and development of network security technologies. He was part of the University of Illinois research team that originally developed the technology that drives the Network Perception Platform. He received his PhD in the field of cybersecurity from the University of Maryland College Park before joining the Information Trust Institute (ITI) at the University of Illinois at Urbana-Champaign (UIUC) as a Research Scientist.

10.30 – 11.00 **Coffee Break**

11.00-12.15 Driving the Utility of the Future: Cyber Policies and Experiences

Moderator: **Melissa Mann, Senior Manager – Cybersecurity and Incident Response, Security & Infrastructure Practice West Monroe Partners**

Discussion panel participants: National Grid, AES and Dominion (invited)

12.15 – 1.15 **Lunch**

1.15 – 1.45 Approaches for Assessing and Interpreting Utility Cybersecurity Postures

The Illinois Commerce Commission (ICC), through its Office of Cybersecurity and Risk Management (C&RM), is actively engaged in assessment of those security approaches taken by investor owned utilities serving Illinois consumers and businesses. How does the Office of C&RM approach interpretation and assessment of ongoing threats to reliability, resiliency and security of the distribution of electric, gas, water and telecommunication critical infrastructure services?

Areas of focus and discussion will include:

- Determining the role of the Public Utility Commissions in cybersecurity across the country;
- Partnerships, collaboration and information sharing activities;
- Approaches taken by C&RM to add value to addressing this evolving area of risk;
- Designing and participating in exercises and active learning opportunities; and
- Determining what the next threat(s) could be and keeping preventable risks from impacting utility service delivery.

Dominic Saebeler, Director, Office of Cyber Security and Risk Management, Illinois Commerce Commission

Dominic focuses on cybersecurity awareness, best practice adoption and assessment of industry capabilities and levels of security preparedness. Dominic researches, writes and presents on challenges associated with addressing cyber risk in critical infrastructure. Dominic is also an adjunct professor at the University of Illinois - Springfield where he lectures on the impact cyber risk has on modern business

decision making. In his almost 30 year career, he has focused on the intersection of policy, security, technology and law. In addition to designing a new state technology agency and various GC and C-level positions at the State of Illinois, Dominic worked in the private sector for 15 years in various roles including technology sales and as an attorney and technology consultant (including seven years at the former Ameritech
(now part of AT&T).

1.45 – 2.15 Protecting Critical Infrastructures from Cybersecurity Threats – What You Need to Know

Modern day industrial operations often span complex IT (information technology) and OT (operational technology) infrastructures. In a very standard environment, thousands of devices exist and are increasingly being connected via the Industrial Internet of Things (IIoT). This creates new challenges in securing industrial environments specifically by making cyber-security threats even more difficult to detect, investigate and remediate. In this session we will address:

- Critical Infrastructure is so much more than you think
- Current industrial attack methods and targets
- Actors and motivations
- What has changed in the threat landscape
- Five key areas to address to secure your IT/OT infrastructure

Michael Rothschild, Director of Marketing, Indegy

Michael Rothschild is the Director of Marketing at Indegy. With a proven track record of 20+ years security and networking, he has a passion for inspiring and motivating world class marketing teams in product and field marketing. Prior to joining Indegy, Michael was the Global Director of Marketing at Thales. Michael occupies a board seat at Rutgers University and has published a variety of works. In his spare time volunteers as an Emergency Medical Technician.

2.15 – 2.45 Modernizing Infrastructure and Securing IT/OT Systems & Data

The energy sector has a significant opportunity for innovation as new connected technologies are integrated into the generation, transmission, and distribution processes; the rise in
deployments of Distributed Energy Resources (DERs) and the Industrial Internet of Things (IIoT) has set the stage for a highly interconnected, reliable, and responsive energy grid. However, the challenge of securing existing grid resources against cyber vulnerabilities created by new technologies is just as significant; this level of increasing interconnectivity has simultaneously made the grid more vulnerable to cyber-attacks than ever before.

Given the mounting security threats to the existing grid, having an appropriate strategy in place to maintain resilient operations through a cyberattack has become paramount. Guaranteeing safe and reliable electricity and gas delivery to customers requires a cybersecurity strategy beyond just compliance with current regulatory guidelines.

Attendee Takeaways:

- Why Operational Technology (OT) may be your Cybersecurity Achilles' Heel
- Grid Modernization Cyber Assessment/Readiness

- Telecom does more than transport data; it can help support the organization's security posture

Scott Crider, Manager-Cybersecurity, West Monroe Partners

Mr. Crider is an experienced Cybersecurity Professional with most recent comprehensive experiences within the Nuclear and Bulk Power Utility, Oil and Gas, Transportation, Clinical Information Systems, and Pharmaceutical/Biotechnology Industries. Focused as a leader in the development of Cybersecurity Programs for Energy and Bulk Power Utility clients, delivering solutions to market leveraging best of breed capabilities within West Monroe Partner's Cybersecurity Consulting Practice. As a Manager, drives out new Business Development opportunities, serves as an Engagement Manager and Energy and Bulk Power Utility Cybersecurity expert with focused understanding of Utility Cybersecurity, Cyber Resilience, and Critical Infrastructure.

Dan Frein, Architect, Technology – Cloud & Infrastructure, West Monroe Partners

Dan Frein is an Architect in West Monroe Partners' Cloud & Infrastructure Practice. He brings over 10 years of experience providing infrastructure competency across many industries, especially the Energy & Utilities industry. Dan's areas of expertise include IT strategy, network design and implementation, and cybersecurity. He is also frequently involved in IT due diligence assessments across a variety of industries. Dan received his Bachelor of Science in Industrial Management (BSIM) from Purdue University; he has also earned several technical IT certifications, including SSCP, CCNP, and ITIL foundations.

Dan continues to work on several Nokia/Alcatel-Lucent MPLS network design and implementation projects for utility clients. These networks provide the segmentation and security measures that are consistent with NERC/CIP requirements to enable utilities to provide scalable and secure transport to SCADA, IT, and other business units in the organization. Most recently, Dan has been helping businesses understand how they can improve operational efficiency and enable rapid growth through leveraging cloud services, assessing the organization's current application landscape for appropriateness within IaaS, PaaS, or SaaS environments.

2.45-3.15 **Coffee Break**

3.15 – 3.45 **Managing Smart-Home IoT Cyber Threats to Critical Infrastructure**

Consumers are rapidly adopting smart-home IoT devices and becoming more engaged in energy generation and management for their homes. As a result, energy networks and consumer networks are becoming much more entangled, changing the ecosystem of cybersecurity threats to critical infrastructure. Smart-home solutions must be protected against cyber security vulnerabilities that could compromise homes and the broader energy networks around them.

Our presentation examines these emerging cyber threats and provides a robust cyber security roadmap based on several international standards and frameworks. We distill these standards into key steps for product manufacturers and provide a model for a practical third-party program energy companies can use to help assure the cyber security of IoT solutions for their business systems and consumer programs.

Eric Richardson, Global Cybersecurity Manager, The CSA group

Eric manages global testing, certification and training for customers focusing on Cybersecurity. Eric has over 25 years of experience in high tech, spending the last twenty years at Microsoft and T-Mobile in leadership roles focusing on security and cybersecurity. Eric has an MBA and is just now completing an MsC in Computer Science/Cybersecurity Engineering and resides in the Seattle area. Eric is a Member of the ISA Security Compliance Institute Technical Steering Committee as well as the IECEE working group on Cybersecurity.

3.45 – 4.15 Reducing Cyber Risks and Optimizing Operations at Remote OT Sites

In the Energy Sector, Operational Technology (OT) including control systems and associated IT interfaces (HMI, EWS, etc..) are located at tens of thousands of remote sites including utilities such as natural gas distribution and electrical substations as well as power generation and transmission locations.

These OT sites typically employ physical security such as cameras, fences, locks, etc…though lack the logical user access visibility and controls that is commonplace in Enterprise IT environments. This lack of logical user access control creates a blind spot which increases operational and cyber risks and can potentially negatively impact general public safety.

This discussion and demonstration will focus on a Utility Case Study showing how employing a simple, secure and NERC compliant user access platform at remote OT sites can help asset owners reduce costs by optimizing remote operations while also mitigating potential cyber and operational risks associated remote site control systems. We will also explore how getting user access analytics and forensics data can help control system operators can assist with training and make better decisions on managing their environment and positively impact public safety.

Bill Moore, Founder and CEO, Xona Systems

Xona provides a unique “zero trust” access platform especially tailored for remote Operational Technology (OT) sites. Bill is currently working on several utility projects to reduce operational costs and cyber risks. Previously Bill was VP of Public Sector business at Hypori where he was responsible for overall GTM public sector strategy, sales and business (channel) development for Hypori’s Enterprise Virtual Mobility Platform.

Prior to Hypori, Bill was one of the first strategic account managers for FireEye (FEYE), working closely with large enterprise customers including Northrop Grumman, Lockheed Martin, Huntington Ingalls, DHS and US State Department. Bill brings more than 20 years’ experience in the high tech industry, including positions in sales, marketing, engineering and operations. He has accumulated extensive experience in developing Public Sector and Utilities business for high growth emerging technology companies. Bill holds a Bachelor’s degree in Economics from James Madison University.