Technology Advisory

NRECA's Cyber Security Summit: A Catalyst for Co-op Discussions about Cyber Security Risks

What has changed?

NRECA's Rural Cooperative Cyber Security Capabilities Program (RC3) held its inaugural Cyber Security Summit in January 2017 to educate co-ops on current and emerging cyber security threats, facilitate peer-to-peer discussions on approaches co-ops are using to address cyber security challenges, and increase awareness of existing cyber security resources. The first Summit was co-hosted by the National Renewable Energy Laboratory (NREL) in Golden, Colorado, and had approximately 75 participants. This was the first in a series of five one-day Summits the RC3 Program will hold across the country.

What is the impact on cooperatives?

Cyber security challenges are increasing for all segments of American society and electric cooperatives are no exception. When a cooperative integrates new software and hardware into existing systems, it often results in modifications and extensions to the cooperative's communications and operational networks. While these changes often offer significant benefits to a cooperative, they can also create new cyber security vulnerabilities, or expand the risks associated with existing cyber security vulnerabilities.

At the same time, cyber-attacks are becoming more sophisticated. The economic incentives for criminal attacks, such as ransomware, continue to drive innovations in malicious intrusion and data theft techniques. Cyber incidents can result in lost productivity and, potentially, service disruption. All co-ops, regardless of size, need to take ongoing steps to ensure the security of their data and operational systems.

The RC3 Program recognizes that cyber security is not an information technology challenge. Like safety, it is a team effort that requires directors, managers, and all the staff across the cooperative to be aware and vigilant to prevent and quickly mitigate incidents. As different staff members work to understand their role in protecting their cooperative, opportunities for peer-to-peer learning enable them to share the approaches they use to address cyber security challenges.

One of the RC3 Program's goals is to facilitate Cooperation Among Cooperatives, and the January 18th Summit exceeded expectations earning praise from participants:

> *"Thanks for making the effort to arrange face-to-face opportunities like this. I get as much out of the side conversations as I do the formal presentations."*
>
> *"Very timely and important topic!"*
>
> *"It made me think much more about collaboration and the possibilities that exist to make it much better."*
>
> *"This is a great forum to share with other IT staff from small co-ops. I hope that something can be started to help those of us with small IT staff."*
>
> *"Information sharing and emerging technologies" were the most valuable insights or takeaways gained at this workshop.*

Maurice Martin, Senior Technology Leader, Cyber-Physical Systems Security & Resilience Center (CPSS&R), National Renewable Energy Laboratory (NREL)

Greg Sparks, President, CIOsource

What do cooperatives need to know or do about it?

The Summits are free and are designed for CEOs and all cooperative staff members who have responsibility for cyber security in their co-op. The information provided at the Summits is for both cyber security staff, and staff with little or no technical expertise in cyber security, from office administrators to billing and finance staff.

The Agenda for the January 18th Summit and copies of the presentations are available on the RC3 website. The exact dates for the next four Summits are not finalized, but the following three locations and dates have been tentatively scheduled:

- April 2017 –Cybersecurity Center for Secure Evolvable Energy Delivery Systems (SEEDS), University of Arkansas, Fayetteville, AR
- May 2017 – Cyber Resilient Energy Delivery Consortium (CREDC), University of Illinois at Urbana-Champaign, IL
- June 2017 – Pacific Northwest National Laboratory, Richland, WA

Final dates and locations will be announced on our member website on cooperative.com and announced via our twice-monthly newsletter to members, *TechUpdate*.

Additional Resources

- NRECA Cyber Security websites:
  - RC3 Website Page
  - Public page
  - Additional resources for NRECA members
- Guide to Developing a Risk Mitigation and Cyber Security Plan
- Sign-up for NRECA's newsletter, *TechUpdate*

The National Renewable Energy Laboratory (NREL) advances the science and engineering of energy efficiency, sustainable transportation, and renewable power technologies and provides the knowledge to integrate and optimize energy systems. NREL's Cyber-Physical Systems Security & Resilience (CPSS&R) center serves as an independent resource for utilities and energy-sector companies to evaluate the security of new technologies and get objective insights on organizational cybersecurity efforts from experts in the field. https://www.nrel.gov/esif/cybersecurity-resilience.html

The Electricity Information Sharing and Analysis Center (E-ISAC) serves as the primary security communications channel for the electricity industry, and enhances industry readiness and its ability to respond to cyber and physical threats, vulnerabilities, and incidents—each of which could cause a potential impact to the bulk power system (BPS). The E-ISAC gathers and analyzes security data, shares appropriate data with stakeholders, coordinates incident management, and communicates mitigation strategies with stakeholders. https://www.eisac.com

Contact for Questions

- RC3 email: CyberSecurityRC3@nreca.coop
- Cynthia Hsu, Ph.D., Cyber Security Program Manager: cynthia.hsu@nreca.coop

This material is based upon work supported by the Department of Energy National Energy Technology Laboratory under Award Number(s) DE-OE0000807.