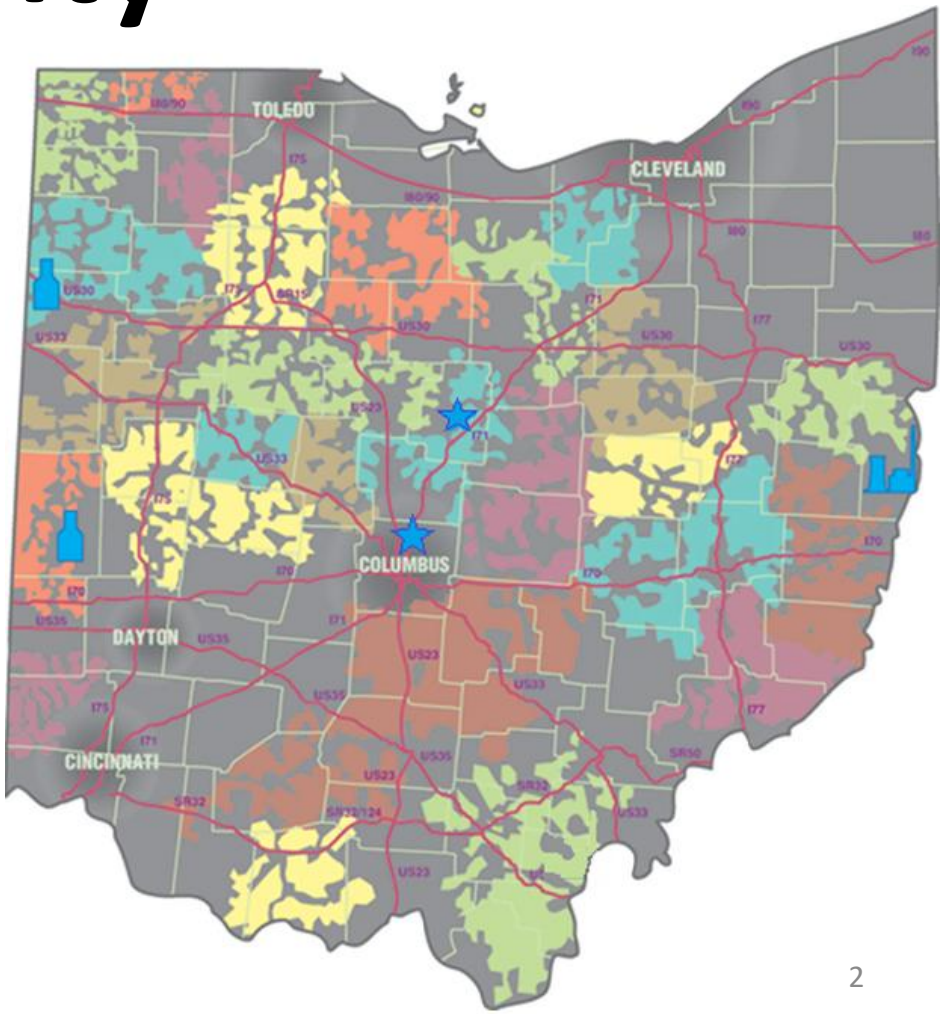
Leadership in Cybersecurity: Safeguarding Co-op Operations

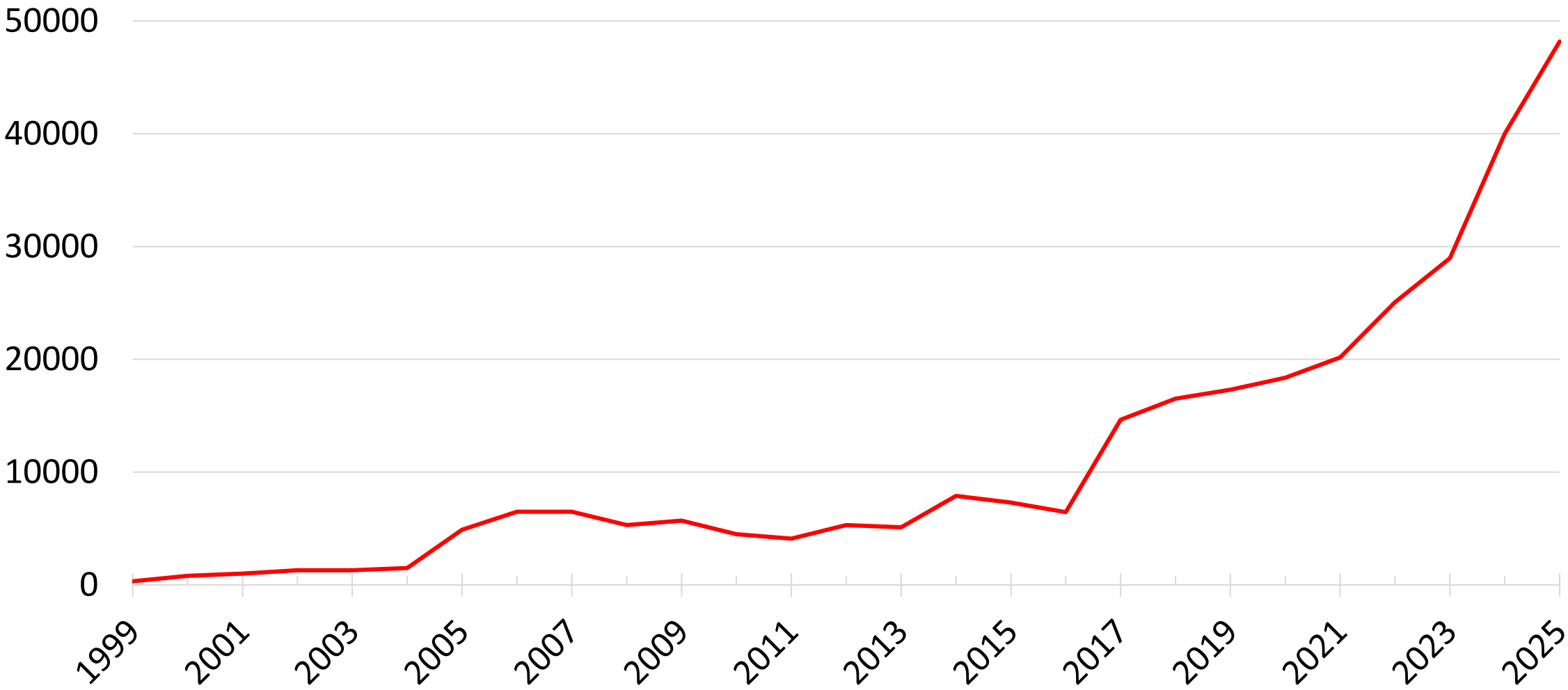
BUCKEYE POWER, INC.
OHIO RURAL ELECTRIC COOPERATIVES, INC.

Cooperative Cybersecurity

- Why is this important?
- How is OEC Statewide supporting your Cooperative?

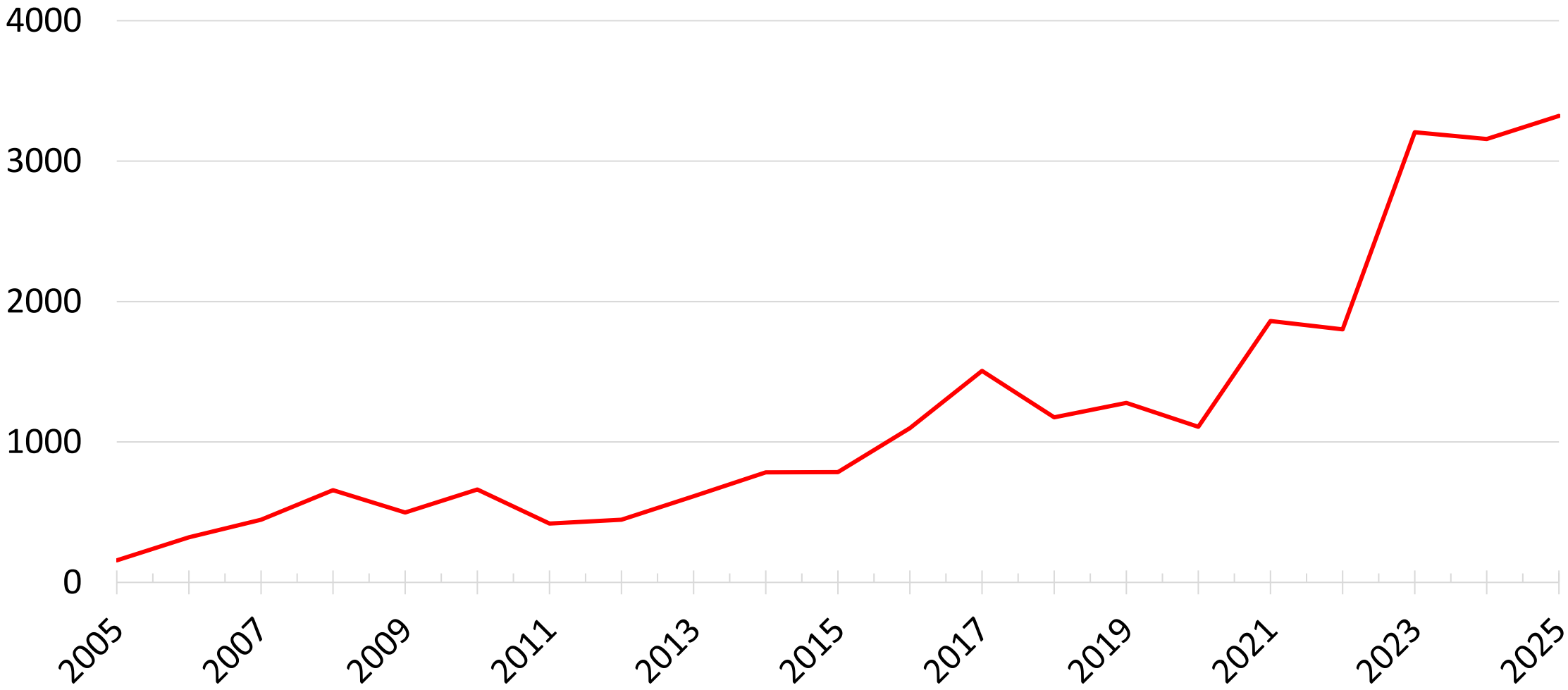


Vulnerabilities Published Annually



www.cve.org

Publicly Disclosed Data Breaches (U.S.)



idtheftcenter.org

sPower
(March 2019)

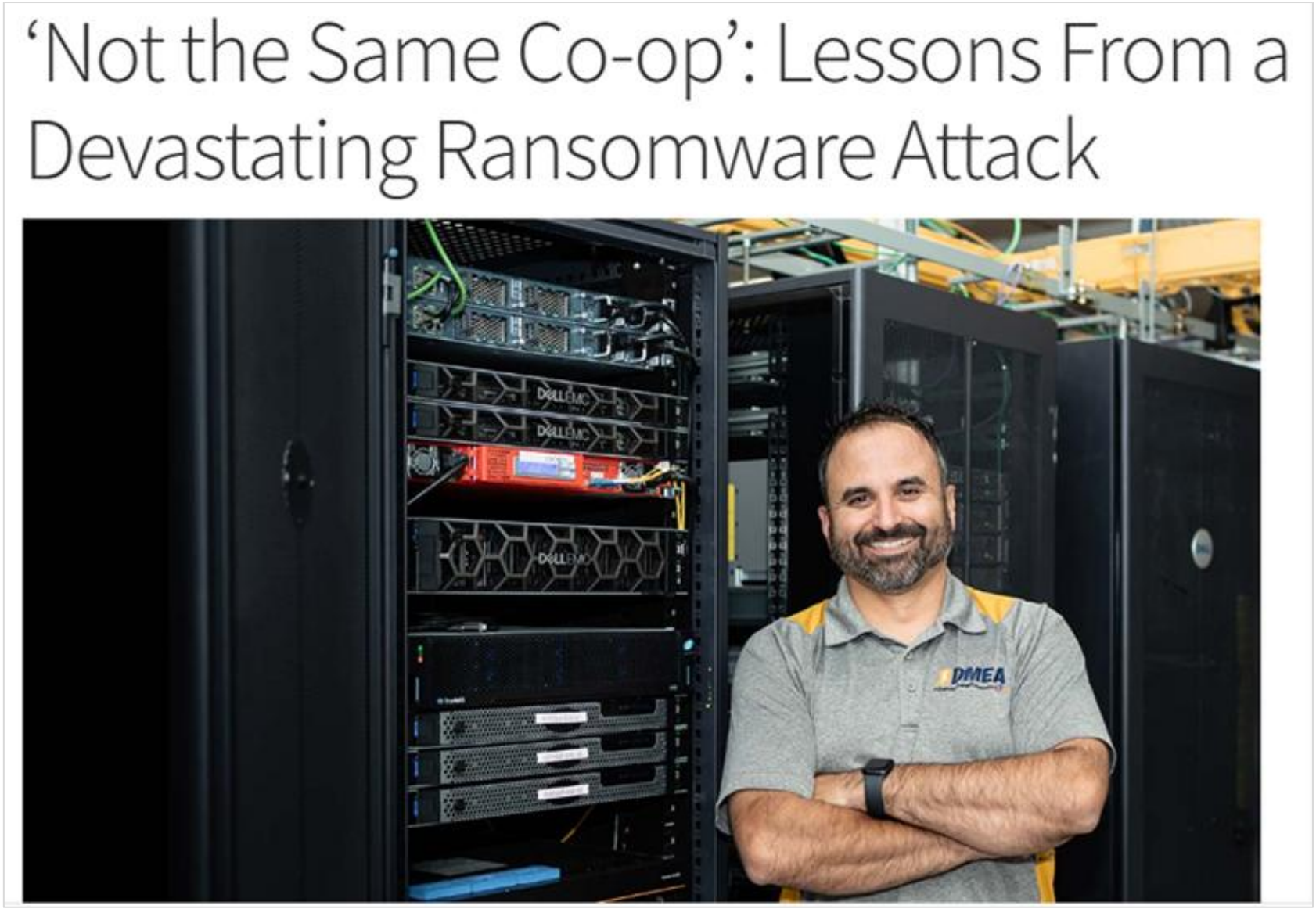
NERC finds first remote hacker interference on US grid from cyberattack

Published Sept. 9, 2019

- The North American Electric Reliability Corporation (NERC) on Wednesday revealed details about a March 5 cyber event that caused an undisclosed utility in the western United States to temporarily lose visibility of certain system parts.

Utility Dive

Delta-Montrose Electric Association
(November 2021)



[RE Magazine, November 2023]

Critical Infrastructure Is Under Attack

Edisto Electric Cooperative Attacked as Helene Descends
September 2024

Qilin Ransomware Attack On Tennessee Valley Electric Cooperative
March 6, 2026

Hackers Hammer Texas Electric Cooperatives in Alleged Ransomware Breach
October 22, 2025

DragonForce Strikes Graham County Electric Cooperative With Ransomware
March 6, 2026

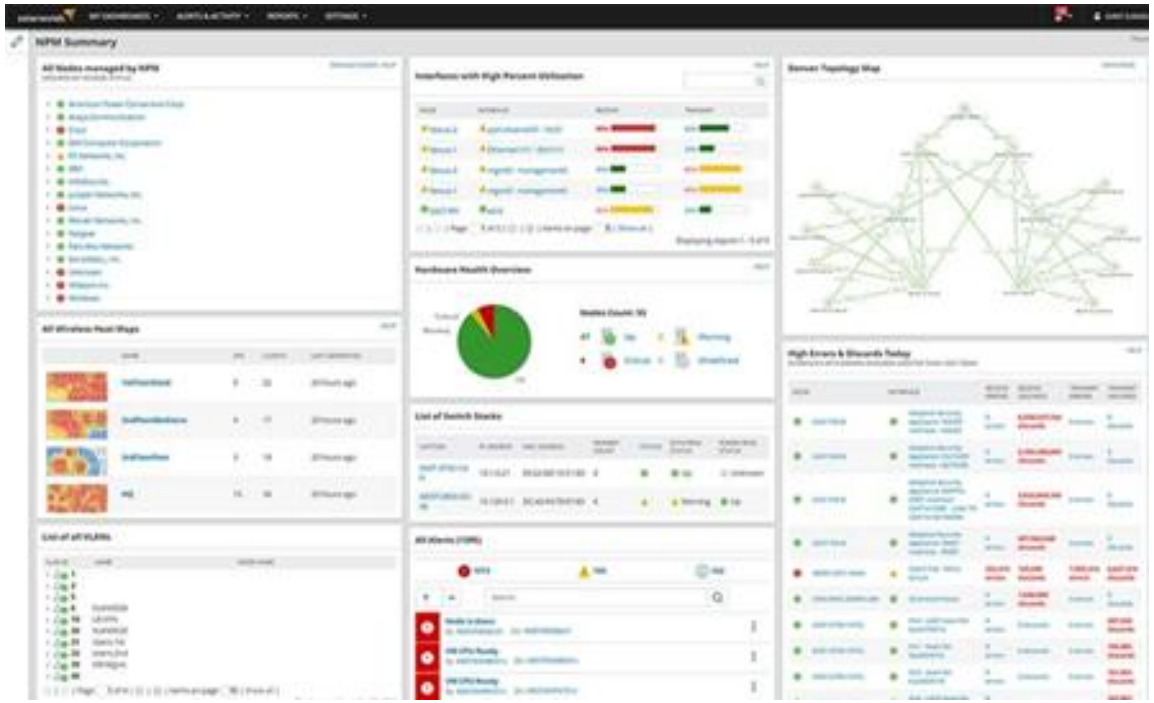
NBC NEWS — *Updated: August 3, 2026*

Hackers targeted municipal water systems in 7 states this week, FBI says
The federal warning comes after more than 30 water facilities in Minnesota were breached.

Major US Utilities Affected by Data Breach — Jan 2026

Cyberattack against US engineering firm allegedly exposes data believed to be related to large US utility companies AEP, Duke Energy Florida, and Tampa Electric Company.

SolarWinds



- Used by >30,000 organizations to monitor IT systems, including 425 of the Fortune 500
- Russian nation-state attackers
- Attack began September 2019, discovered December 2020
- **Supply chain attack - the targets were SolarWinds' customers**
- Fewer than 100 customers compromised, but included Microsoft, Intel, Cisco, AT&T, Deloitte, Lockheed Martin, US Justice Department, US State Department, US Treasury Department, Pentagon, and NASA

Zero-click Attacks

- **Google Gemini (2025) and ChatGPT (2025)** - hidden malicious instructions embedded in Gmail, Google Calendar, and Google Docs; automatically executed as legitimate actions *(Symantec)*

- **WhatsApp and Apple iOS/macOS devices (2025)** – compromised WhatsApp communications on Apple devices *(The Hacker News)*

- **iMessage (2019 - 2024)**: ***Pegasus*** and ***Operation Triangulation*** zero-click exploits to compromise iPhones *(BleepingComputer)*.

How Can We Protect Our Cooperative?

- Safety is everyone's job, and so is cybersecurity
- Cover the basics
- What are we missing?
- Invest in your People, Process, and Technology

Rural Electric Cyber Advancement Program (RECAP)

OEC Program History:

RECAP
RURAL ELECTRIC CYBER ADVANCEMENT PROGRAM

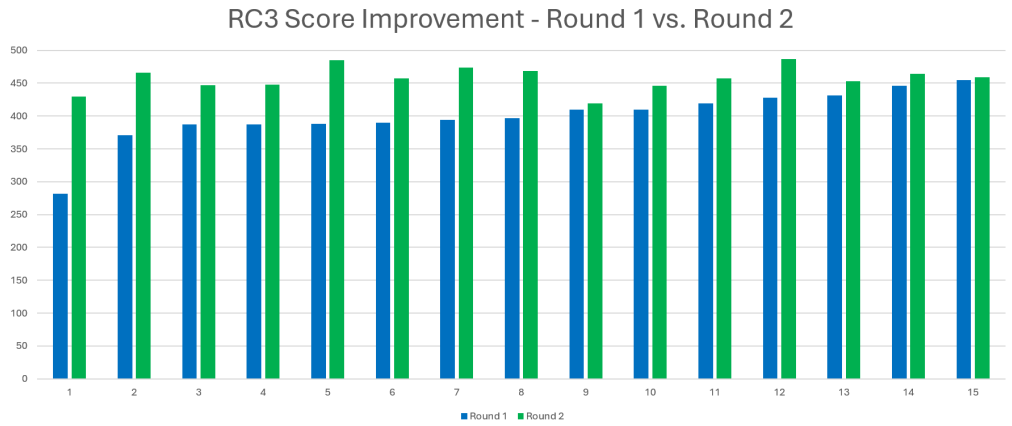
2020 – NRECA RC3 tool procured

2021 – Cyber Assessments begin

- Lessons Learned from other co-ops
- Based on RC3 assessment tool
- Performed every two years
- OEC facilitator; OEC & member SMEs

2024 – Program Expansion

- Member driven
- Dedicated RECAP staff
- More visits, new services

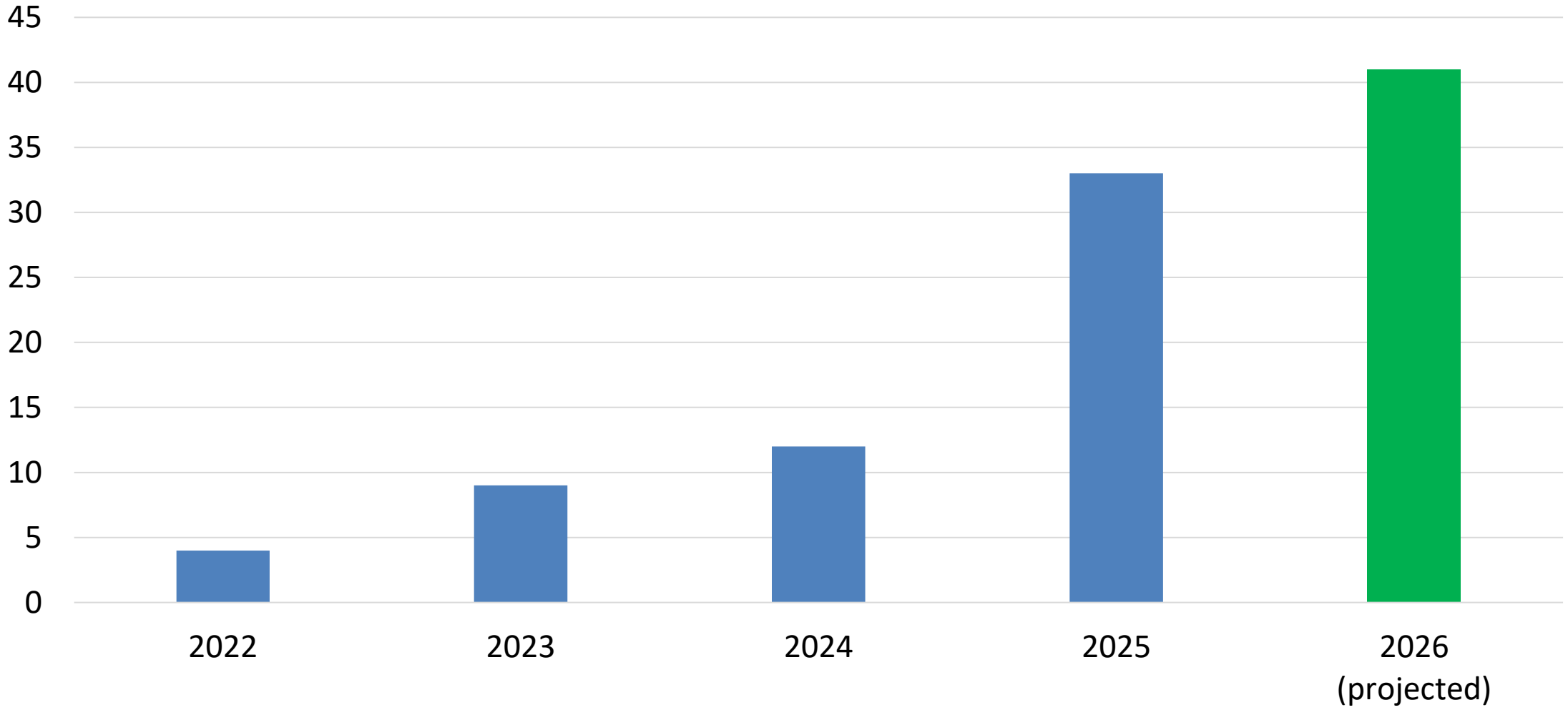


OHIO'S ELECTRIC COOPERATIVES
Your Touchstone Energy® Cooperatives

BUCKEYE POWER, INC.
OHIO RURAL ELECTRIC COOPERATIVES, INC.

RECAP
RURAL ELECTRIC CYBER ADVANCEMENT PROGRAM

Total Onsite Visits for RECAP Services

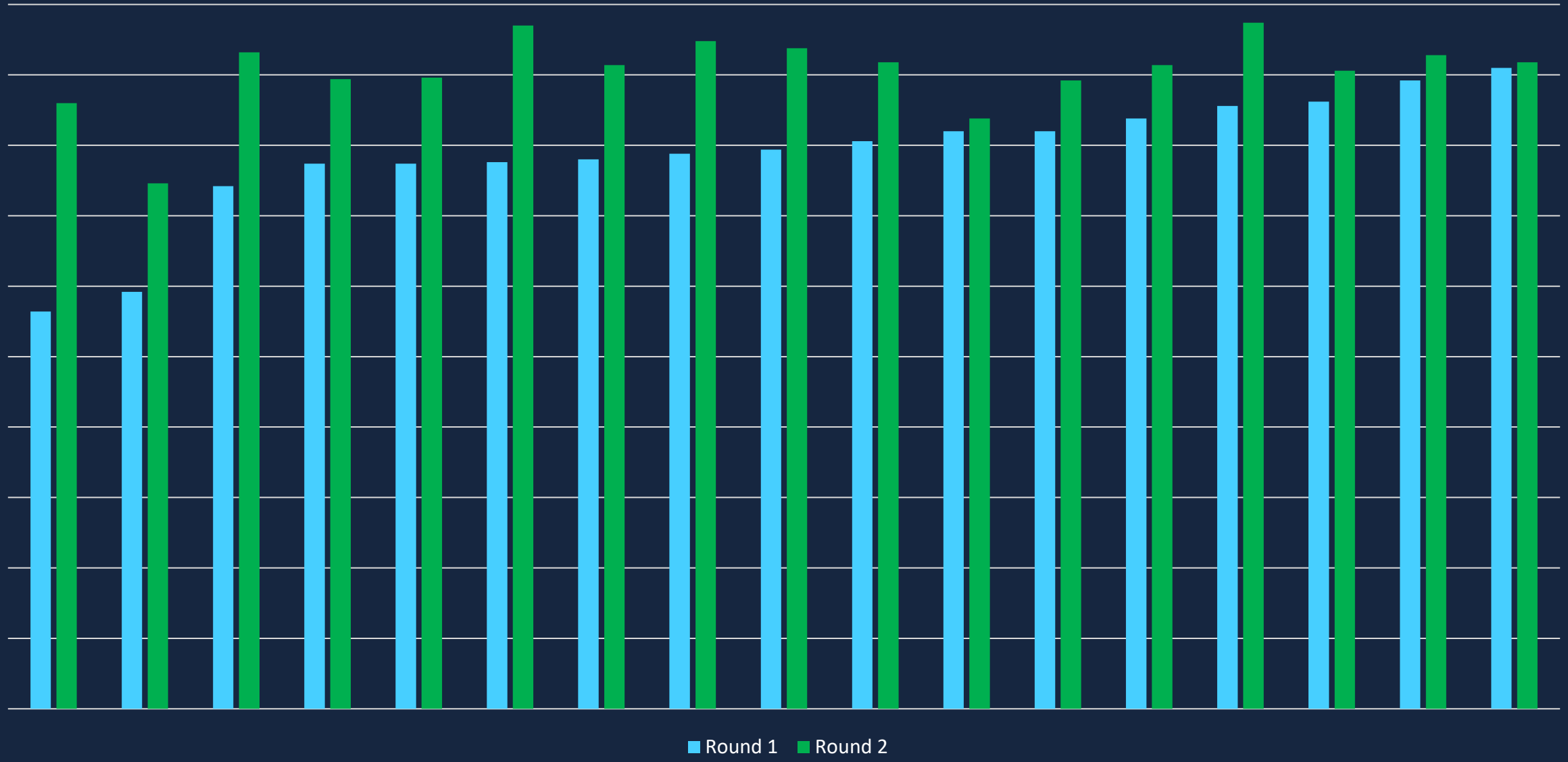


RECAP

RURAL ELECTRIC CYBER ADVANCEMENT PROGRAM

OEC 2026 Summer Conference

Rural Cooperative Cybersecurity Capabilities (RC3) Scores



RC3 Assessment Evolution

Expanding our risk assessment to address the modern threat landscape

Round 2

OSINT Report – Scan of external network perimeter and analysis of co-op social media information leakage.

Average Result Increased from 78.11% (C+) to 91.50% (A-)

Round 3

New Documentation Standard

New and Updated Questions Covering Newly Emerging Security Domains

New Documentation Standard

☑ Pre-Assessment Checklist

- ❑ Network Asset Inventory (IT &OT)
- ❑ Network Map (IT & OT)
- ❑ Member Mobile Device Inventory
- ❑ Building & Property Inventory
- ❑ Inventory of IT, OT, and Cloud Devices that Store Sensitive Information
- ❑ Latest IT & OT Risk Assessment
- ❑ Latest IT & OT Vulnerability Assessment
- ❑ Latest Cloud Tenant Security Reports
- ❑ Partner/Third Party Provider Background Check Policies
- ❑ Physical Security Plan
- ❑ List of Cybersecurity-related Responsibilities Important to the Cooperative
- ❑ Cybersecurity Policies
- ❑ List of Cybersecurity Information Sharing Resources Used by the Cooperative
- ❑ List of Cybersecurity Responsibilities Delegated to Partners/Third Party Providers
- ❑ List of Partner/Third Party Provider Employees with Unsupervised Remote Access (IT & OT)
- ❑ Documentation of Partner/Third Party Provider Security Track Records and Assessment History
- ❑ Documentation of Internal Cybersecurity Framework used by Partners/Third Party Providers
- ❑ Log Review Process
- ❑ Date of Last Firewall Rule Review
- ❑ CIRP (Cyber Incident Response Plan)
- ❑ ERP (Emergency Response Plan)

New Assessment Domains

Five critical areas now integrated into the RC3 framework

Shadow IT

Discover and govern unauthorized applications, cloud services, and personal devices across the enterprise

OT Monitoring

Deploy continuous visibility and segmentation controls across operational technology networks

Cloud Config

Audit identity, access, encryption, and security defaults across cloud tenants

AI Use

Establish acceptable use policies and risk controls for generative AI and copilot tools

DLP

Classify sensitive data and enforce loss prevention policies across endpoints and cloud

New Service Offerings (3/year)

Tabletop Exercises

- Supply Chain Ransomware Attack
- Nation-state SCADA Attack
- New Topic TBD (10/26)

Training

- General Staff
  - Cybersecurity Basics
  - Social Engineering
  - AI Use and Security
- Technical Staff
  - IT/OT Segmentation
- Board Briefings

Assessment Review

- Development of new policies from tested templates (AI, CIRP, Acceptable Use, Cybersecurity Program)
- Analysis of existing policies' completeness and appropriateness

Policy Review

- Review policy gaps identified in previous RC3 assessment
- Discussion of remediation strategies and any challenges to continued progress

Future Possibility – Risk Assessment?

Upcoming RECAP Visits

	T1 2026	*T2 2026*	*T3 2026*
Co-op 1	Assessment	Policy Review	Training
Co-op 2	Assessment Review	Board Threat Briefing	Tabletop Exercise
Co-op 3	Tabletop Exercise	Training	Assessment
Co-op 4	Policy Review	Tabletop Exercise	Assessment Review

State & National Engagement

Ohio Comprehensive Cyber Plan Planning Committee

- Guide long-term direction for how Ohio prepares for, responds to, and manages cyber risks across all levels of government and critical infrastructure
- Share threat experience across disparate fields to strengthen Ohio's overall Cyber resilience
- Guiding document, not authority or direction over local entities

State & National Engagement

NRECA Project Guardian Cyber Champion

- "Identify, replicate, and scale successful cybersecurity efforts and programs within cooperative utilities focusing on cybersecurity awareness, services, guidance, and collaboration in a specific area or region"
- Twelve members nationally
- OEC's RECAP one of three cybersecurity programs presented as model to emulate during inaugural Cyber Champion meeting (November 2025)
- OEC used as one of two testbeds for new "Cyber Sync" program
- OEC participated in Co-op Cyber Tech general session panel: "How Co-ops Are Turning Strategy into Defense"

Other RECAP Services

- Cybersecurity Office Hours

  Monthly open forum for OREC IT staff to ask questions and discuss the efforts and challenges they're facing

- Cyber Threat Monitoring

  Information sharing with IT Manager's association

- IT Manager's association Technology Survey updates
- IT Staff onboarding assistance for OREC members

Current Threat Landscape

Iran Conflict

- Increased frequency of Iranian-supported cyber-attacks
- Critical Infrastructure is a frequent target

Current Threat Landscape

Mythos – The Risk of AI Hacking

Claude Mythos is pre-release LLM created by Anthropic. It has been made available to 11 organizations to check their software for vulnerabilities before Mythos is publicly released.

- Mozilla discovered 271 new vulnerabilities in Firefox
- Mythos was able to defeat an “expert” level cyber range challenge, finding a 32-step path to full network compromise.
- There’s every reason to believe its release will cause a flood of zero-day vulnerabilities in organizations without pre-release access. If more organizations are given early access to future pre-releases, chances of a bad actor getting access increase with it.

Current Threat Landscape

Increasing Online Threats to Field Equipment

E-ISAC has noticed a dramatic uptick on threats against the Energy sector being made online. These are often tied to displeasure with the increase in AI data centers, noting that security around equipment like substations is often lower than the data centers themselves, e.g.

> “you don't blow [the data centers] up, you fly drones trailing mylar tape over the substations that feed them. The infrastructure that powers them is unironically both a softer target and more expensive to replace than the data centers themselves.”

Current Threat Landscape

Increasing Online Threats to Field Equipment

Current attacks are rare, but not unheard of. This could change quickly if such attacks become “viral”. When that will happen is hard to predict.

Ensuring adequate monitoring around valuable, unmanned assets is recommended before that happens.