NRECA
America's Electric Cooperatives

CO-OP

CYBERSECURITY

Special Report

First Published in the November 2023 Issue of *RE Magazine*

A WORD FROM NRECA'S DIRECTOR OF CYBERSECURITY

As modern innovations continue to revolutionize the way electric cooperatives can serve their communities more efficiently and more reliably—including things like new grid devices, cloud migration, microgrids and IT/OT collaboration—they also present new challenges for cybersecurity.

Co-op data and systems are attractive targets for cybercriminals, whose tactics and techniques change constantly. But there are ways to fortify networks, processes and culture to mitigate risk.

In this special report, which was first published in the November 2023 issue of *RE Magazine,* we take an in-depth look at how one co-op responded to a devastating ransomware attack and how it came back from the incident stronger. We also highlight a trend among electric co-ops, their statewide associations and their G&Ts to join forces to strengthen end-to-end defenses against cyberthreats.

We've included a detailed infographic to help you visualize the universe of cyber risks for co-ops, as well as a look at NRECA's Co-op Cyber Goals Program and advice on managing the security of third-party systems and devices.

Our unique culture of sharing information and resources and collaborating to elevate all co-ops is an enormous advantage in this fight. I hope you find this special report insightful, useful and a call to action to make sure your co-op has done all it can to protect your members and safeguard your systems.

Carter Manucy
Director, Cybersecurity

Cover Image by BlackJack3D/Getty Images

TABLE OF CONTENTS

Lead Story: A New DMEA | **2**

Feature: Statewide and G&T Cyber Help | **6**

Infographic: Cyberthreats and Defenses | **8**

Feature: Cyber Goals | **10**

Feature: Contract Review | **12**

Meet our Team | **13**

Resources, Opportunities and Contacts | **14**

Stories by Cathy Cash, NRECA Communications

IT Manager Jay Suckey, who has been with Delta-Montrose Electric Association since 2017, helped guide the co-op through a cyberattack in late 2021 that shuttered critical systems and took about four months to recover from. DMEA is sharing its story and lessons learned with other co-ops.

‘NOT THE SAME CO-OP’

A co-op’s lessons learned from a devastating ransomware attack

“This was my boom.”

Jay Suckey has the sinking feeling memorialized in a chat message he saved from 5:13 a.m. Sunday, Nov. 7, 2021: A Delta-Montrose Electric Association dispatcher couldn’t log in. Suckey, DMEA’s system administrator at the time, also was denied access.

It would soon become clear that the Montrose, Colorado-based co-op’s systems were in the middle of a highly invasive cyberattack, a boom that would alter the co-op forever.

Suckey, now DMEA’s IT manager, and Chief Information Officer Bob Farmer told the gut-wrenching tale and accompanying four-month comeback at the NRECA 2023 Co-op Cyber Tech conference.

As DMEA moves toward full recovery, the two IT professionals are sharing their story as a warning for co-ops to bolster their cyberdefenses to stay left of boom and to provide tips on recovery should disaster strike.

“We are not the same co-op,” says Farmer. “We’re an improved and more secure DMEA because of it.”

BOOM!

The ransomware text message outlined the damage done and the potential for more with no option for recourse. In 18 minutes, the hacker had taken down DMEA’s phone and email system and its customer management platform while also disabling the meter data management system, mapping system, file servers and active directory.

DMEA's backup files were stored offsite miles away but not off network. They were obliterated.

The IT team called the CEO, who informed the board president. They then reported the attack to state and federal authorities, including the FBI and the Department of Homeland Security. They also contacted their primary technology vendor, NISC.

> "By telling our story, we hope others share their own incidents and near misses. Each one offers valuable lessons learned, and if co-ops are willing to share, we will all be safer for it."
>
> —Bob Farmer, Chief Information Officer, Delta-Montrose Electric Association

The hacker likely penetrated a single server that had yet to receive the latest security patch. From there, the domain administrator's login information was stolen, and the attack escalated to "data annihilation," Suckey says.

In the days and weeks that followed, the co-op learned a "new normal." Recovery was a moving target, dynamic rather than linear—and at times unknowable.

"There wasn't a 'We will be back to normal on such and such day,'" Suckey says. "It was, 'This is the new way that this will work' because most systems and processes needed to be rebuilt from the ground up."

CRAWLING FROM THE WRECKAGE

DMEA's electric and broadband services never shut down from the attack, but system operations for the co-op initially functioned at a base level and did not resume full operation until mid-December 2021.

Automated integration between the meter data management system and the customer information system was not restored until January 2022. DMEA initially used the paper service territory maps on its dispatch department walls to track service outages while its outage management system was offline.

Billing was the biggest challenge. Without the ability to grab data off members' meters, DMEA was unable to send out invoices for November 2021.

"If your meter data management system is down, that means you're not getting any of the reads from your meters," says Farmer. "Think about how important billing is for a co-op to survive, and how dependent billing is on meter reads."

Customer service reps took over data entry, while other staff, including the CEO, worked shifts on the phones. Data entry carried on until the billing was restored at the end of the year.

Basic phone service was up and running by the end of the week, but DMEA's full phone server wasn't restored until December. A new cloud-based email system was deployed within several days.

As word of the attack got out, members began flooding the co-op with calls. Staff worked to ensure they had the most accurate and up-to-date information to provide to members about recovery efforts.

"What do you tell the members, and when do you tell them?" says Farmer. "My

Photo by Kevin Martins/DMEA

encouragement would be for co-ops to think about that topic in advance and be prepared ahead of time."

The overall cost of the cyberattack is difficult for DMEA to quantify, but it involves lost productivity, temporary reputational harm, new equipment purchases and lots of staff overtime.

Suckey recalls several weeks of coming home from the co-op after his kids were already in bed and then leaving in the early morning before they woke up.

"The emotional impact is way more than we realize," says Farmer. "I have been impressed with how resourceful and resilient DMEA's employees are, but an event like this certainly takes its toll."

'DON'T GO IT ALONE'

Farmer and Suckey say they learned a lot being "right of boom." First and foremost, "Don't go it alone. Don't reinvent the wheel. And be open to feedback."

Fortunately, DMEA had a cyber insurance policy that included an incident response team to launch its own investigation and recovery efforts.

"Insurance is not a magic fix-all, but it is a huge help during the incident, and it helps you to recover to your new normal," says Farmer.

In the wake of the attack, the co-op's CEO also hired a third-party cybersecurity firm, which remains a trusted technical partner today.

DMEA is making use of many of the co-op cyber tools and programs offered by NRECA and participates in tabletop exercises fairly frequently now. That includes some of the most significant cyber drills hosted by NRECA, plus the biennial GridEx held by the North American Electric Reliability Corp.'s Electricity Information Sharing and Analysis Center (E-ISAC).

"Tabletops are a huge help by allowing you to prepare for cyber or physical security incidents," says Farmer. "They allow you to recognize where you have gaps in your existing plan or when you lack plans entirely. Tabletops provide us with the forum for necessary practice to be ready to better respond to the next incident."

DMEA also constantly measures its cyber performance against a host of assessments. That's where it helps to accept the need for better solutions, Suckey adds.

"From the perspective of living through this, the only way that we're going to learn and grow is to have an open mind and focus on improving ourselves and our organization."

The co-op has since improved its vulnerability management and patching process with tools for timely automatic upgrades of devices, including iPads and iPhones.

DMEA has started to focus on the nontechnical side of cybersecurity, such as crafting a cyber incident response plan and an IT disaster recovery plan and updating applicable board and administrative policies.

"We've gone as far as creating an acceptable use policy for our board to protect them while they use our technology," says Farmer. "We appreciate their ability to provide valuable feedback and support for our cybersecurity efforts."

STORY OF WARNING

Sharing DMEA's story isn't easy, say Farmer and Suckey, but they're driven to tell it based on the principle of cooperation among cooperatives. CEO Jack Johnston's belief in the cooperative principles encourages DMEA to continue to keep cybersecurity at the forefront and share its message with others, they said.

"When Jack joined us in January 2023, he certainly could have said, 'It's time to move on, let's forget this happened,'" says Farmer. "Instead, he has embraced it and allowed us to share this important message."

DMEA hopes that destigmatizing the cyberattack it endured will lead to greater willingness among co-ops to talk about threats, preparedness and response and will make everyone safer in the long run.

"We hope that no other co-op goes through what we went through," says Farmer. "By telling our story, we hope others share their own incidents and near misses. Each one offers valuable lessons learned, and if co-ops are willing to share, we will all be safer for it."

DMEA'S TAKEAWAYS

Delta-Montrose Electric Association offers several pieces of cybersecurity advice after recovering from a highly disruptive ransomware attack:

Invest in cybersecurity resources:

- Engage a trusted cybersecurity partner or hire a dedicated expert.
- Take advantage of the NRECA Cybersecurity Program tools and exercises.
- Train your staff using diverse methods, from onboarding sessions to regular drills.
- Buy cyber insurance.
- Implement robust cybersecurity tools for device management and patching.
- Join cybersecurity organizations like E-ISAC to keep informed.
- Engage DHS's Cybersecurity and Infrastructure Security Agency for resiliency reviews.
- Attend and actively participate in state, regional or national cybersecurity conferences.

Think like a hacker:

- Undergo frequent assessments and penetration tests to learn your co-op's vulnerabilities, then work to fix them.
- Disconnect or "airgap" your backup files and ensure they are immutable and cannot be modified or deleted.
- Require multifactor authentication (MFA) for any access to your network.
- Learn the latest threats through your statewide or E-ISAC.
- Draft and update an incident response plan and a crisis communications program.

Break down silos:

- Share experiences of cyberthreats and incidents with colleagues.
- Communicate cybersecurity threats and activities openly and regularly with your board.
- Foster a cyber-safe environment where raising questions and concerns is encouraged.
- Encourage cyber knowledge-sharing across the organization to promote awareness.
- Remember, "the way things have always been done" may no longer be the best or safest way.

Association of Illinois Electric Cooperatives
A Touchstone Energy® Member

Statewide cybersecurity professionals, like Dan Gerard of the Association of Illinois Electric Cooperatives, can be significant resources to co-ops in ways that go well beyond incident response.

Photo courtesy Association of Illinois Electric Cooperatives

'WELL-POSITIONED TO HELP'

G&Ts, statewides, large co-ops offer cyber services to co-ops

A statewide cybersecurity professional can serve as a significant resource to electric cooperatives, not the least of which is being the go-to when cyber hits the fan.

Dan Gerard, chief technology officer at the Association of Illinois Electric Cooperatives, recalls when a co-op CEO contacted him during a cyberattack.

"He wanted me to report the incident to the FBI so the co-op could quickly work with its response team," says Gerard. "I was able to act as a buffer to help free them up."

Statewide associations, professionals at generation and transmission providers and even large co-ops can bolster co-op cybersecurity efforts in ways beyond incident response, including:

- Facilitating self-assessments to identify vulnerabilities.
- Educating staff on security from phishing to identity theft.
- Informing boards of necessary security resources.
- Serving on state, regional or federal panels.

- Tracking federal and state cybersecurity requirements.
- Coordinating group purchasing discounts.
- Offering a fresh set of eyes on nagging cyber issues.

"There's a huge push right now to increase the cybersecurity posture of our critical infrastructure systems," says Gerard, a nine-year veteran at the statewide in Springfield. "As a statewide, we're very well-positioned to help our members."

Gerard also helped form a co-op cyber mutual aid group that's "very similar to what we do for storm restoration," he says.

Kansas Electric Cooperatives hired Bill Glynn in 2022 to be its first cybersecurity director. Glynn came from the Kansas Intelligence Fusion Center after nearly 40 years at an investor-owned utility. He is a point of contact with authorities for co-ops during cyber incidents and a consultant.

"It's a great situation where each of the co-ops can have a piece of my time as they need it, whether they have a dedicated cyber person or they're small and in need of reinforcement," says Glynn. "This position is beneficial to all."

New Horizon Electric Cooperative, a G&T based in Laurens, South Carolina, hired Hal Stone as its first vice president of Information Security in 2021. After an IT career at Clemson University, Stone now teaches a cyber course for co-op staff to "spread the message that cybersecurity is not just an IT problem."

Stone visits co-ops to build relationships for strong collaboration on cybersecurity and evaluates their technologies, processes and procedures to guard against cyber-threats. "I want them to see me as an extension of their team,'" he says.

Associated Electric Co-op Inc., the Springfield, Missouri-based generation provider, created "Cyber Dome" in 2021 to provide round-the-clock service "from a central location, which allows it to centralize the majority of the costs and talent," says Toby Schaefer, Associated's senior manager for cyber operations.

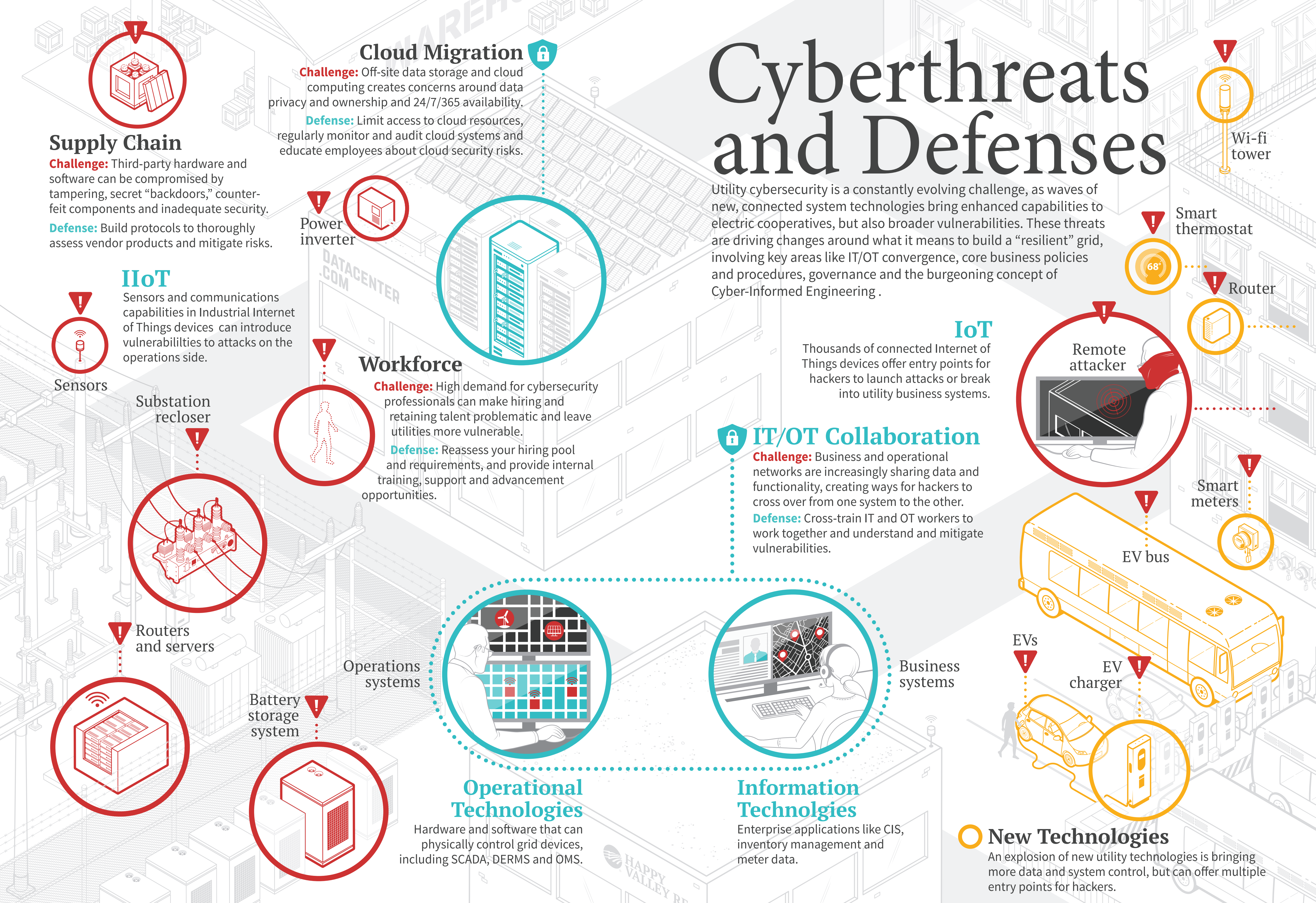
"We provide for our cooperatives protection, detection and incident response," he says. "Cyber Dome monitors cybersecurity environments 24/7/365 and helps coordinate a response from all three tiers—Associated, the G&Ts and the cooperative staff—to any threats in real-time."

Rappahannock Electric Cooperative, based in Fredericksburg, Virginia, formed an IT & cybersecurity subsidiary in 2022 after a significant investment in bolstering the co-op's own cybersecurity posture. BrilliT has 40 employees with eight dedicated cybersecurity professionals and three certified ethical hackers to provide assessments, strategies, data analytics and technologies.

"Being able to provide those services to other co-ops really grew out of the fact that we wanted to ensure that Rappahannock was very well protected," says Peter Muhoro, chief strategy, technology and innovation officer at REC and and BrilliT's general manager. "We've taken it to the next level by saying, how do I help another electric co-op? Because, as infrastructure becomes more and more critical, we truly believe that an attack on one co-op will slowly become an attack on all of us."

Cyberthreats and Defenses

Utility cybersecurity is a constantly evolving challenge, as waves of new, connected system technologies bring enhanced capabilities to electric cooperatives, but also broader vulnerabilities. These threats are driving changes around what it means to build a "resilient" grid, involving key areas like IT/OT convergence, core business policies and procedures, governance and the burgeoning concept of Cyber-Informed Engineering .



Supply Chain

Challenge: Third-party hardware and software can be compromised by tampering, secret "backdoors," counterfeit components and inadequate security.

Defense: Build protocols to thoroughly assess vendor products and mitigate risks.

Cloud Migration

Challenge: Off-site data storage and cloud computing creates concerns around data privacy and ownership and 24/7/365 availability.

Defense: Limit access to cloud resources, regularly monitor and audit cloud systems and educate employees about cloud security risks.

IIoT

Sensors and communications capabilities in Industrial Internet of Things devices can introduce vulnerabililties to attacks on the operations side.

Workforce

Challenge: High demand for cybersecurity professionals can make hiring and retaining talent problematic and leave utilities more vulnerable.

Defense: Reassess your hiring pool and requirements, and provide internal training, support and advancement opportunities.

IoT

Thousands of connected Internet of Things devices offer entry points for hackers to launch attacks or break into utility business systems.

IT/OT Collaboration

Challenge: Business and operational networks are increasingly sharing data and functionality, creating ways for hackers to cross over from one system to the other.

Defense: Cross-train IT and OT workers to work together and understand and mitigate vulnerabilities.

Operational Technologies

Hardware and software that can physically control grid devices, including SCADA, DERMS and OMS.

Information Technolgies

Enterprise applications like CIS, inventory management and meter data.

New Technologies

An explosion of new utility technologies is bringing more data and system control, but can offer multiple entry points for hackers.

The first 20 electric co-ops achieving NRECA's 10 Co-op Cyber Goals were recognized at the 2023 Co-op Cyber Tech Conference in May in Kansas City. The voluntary program helps co-ops set a baseline defense against cyber threats.

Photo by Jeff Peak/Line Creek Media

CYBER GOALS

Co-ops boost defenses and gain 'side benefits'

Electric cooperatives that have completed NRECA's Co-op Cyber Goals say they not only build stronger cyberdefenses but gain a trove of "side benefits," including enhanced collaboration, that can go a long way in improving their cyber posture.

Central Electric Power Cooperative, a G&T based in Jefferson City, Missouri, brought seven of its distribution co-ops along as it met each of the 10 cybersecurity goals in 2023. CEPC is one of more than 50 co-ops to reach the achievement by the end of January 2024.

"Every employee is part of our cybersecurity," says Danny Wortmann, CEPC vice president of information technology. "If you've experienced good collaboration on anything you've done, you know that fosters growth and improvements in other areas that weren't the original intent. Our good working relationships have gotten better between our departments. That's a great side benefit from meeting these goals."

The NRECA Cybersecurity Program launched the initiative in January 2023 to motivate and guide co-ops, no matter their size, toward a solid baseline of cybersecurity by fulfilling the following goals:

LEVEL ONE CO-OP CYBER GOALS

GOAL 1:
Establish a Cybersecurity Point of Contact

GOAL 2:
Self-Assessment

GOAL 3:
Contract Review

GOAL 4:
Multifactor Authentication

GOAL 5:
Default Password Policy

GOAL 6:
Leadership Training

GOAL 7:
Employee Training

GOAL 8:
IT/OT Segmentation

GOAL 9:
Cyber Incident Response Plan

GOAL 10:
Data Backup

Level Two Co-op Cyber Goals coming in 2024. Visit cooperative.com for more information.

When NRECA unveiled the program, CEPC was already well on its way to completing many of the goals, says Wortmann. But clarifying IT's and OT's cybersecurity roles and responsibilities and drafting a cyber incident response plan were challenging.

The G&T, which also provides IT services for its distribution member co-ops, found that having these tasks on NRECA's list—goals 8 and 9—served "as the driving force" to accomplish them, and collaboration was key, he says.

"We didn't come in and say, 'You're gonna do this,'" says Wortmann. "We came in and explained, 'Here's the idea; here's why it is important. Tell us how that would impact you. And are there other ways we could accomplish that?'"

"In the end, OT came up with some ideas that we weren't aware of because we're not living in their world, and we helped them validate that it would meet the goals. It was a good result."

CEPC was one of 20 co-ops recognized at the 2023 NRECA Co-op Cyber Tech Conference in May for achieving all 10 of the Level One goals. Successful co-ops receive a challenge coin and a digital badge to display on websites and social media.

Wortmann advises co-ops pursuing these goals to remember they don't have to reinvent the wheel.

"Make sure you take advantage of any available resource that might help you through this process," he said. "NRECA definitely has some resources that can guide you down the path."

Participate in NRECA's Cyber Goals Program to advance your cybersecurity preparedness. Sign-up at: **www.cooperative.com/cybergoalsprogram**.

THIRD-PARTY VENDORS AND CYBERSECURITY

Staying cybersecure means more than educating cooperative staff. Ensuring that policies and trainings also cover contractors, vendors or managed service providers with access to operations systems and member data is critical to well-rounded security strategy.

"Any third party is a potential vector for a cybersecurity attack," says Nick Pascale, NRECA's deputy general counsel. "To help protect this front, all co-op third-party contracts should include cybersecurity requirements to prevent a breach and clearly defined procedures to ensure full cooperation if a security incident occurs."

To start, co-ops should install onboarding procedures for these third-party contractors to screen for cybersecurity requirements, like the following:

- A commitment to work within your co-op's security policies and practices.
- Verifiable information on their ability to uphold cybersecurity, including documented security policies and procedures and certified proof of test results.
- Information on their mitigation efforts to address past data breaches or cyber incidents.

Illustration by Andranik Hakobyan/Getty Images

Before a contract is signed, co-ops should consider working with their attorney when reviewing and negotiating and ensure the terms include:

- Provisions verifying a clear understanding of how personal data and confidential information are handled and the level of security in place to protect the co-op.
- Sufficient documentation on the business reasons for any contractor to access the co-op's system.
- Processes to ensure accounts made for contractors are unique and secure and that they are disabled when personnel change.
- Nondisclosure agreements with third parties to protect information about your co-op that is confidential or sensitive when contracts end.

After a contract is signed, Pascale recommends that co-ops conduct regular cybersecurity checks with the contractors' operations and systems. It is also important to hold drills after major system upgrades or reconfigurations to ensure procedures are up-to-date, he adds.

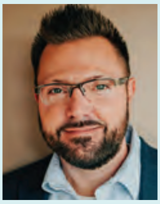
"Strong contracts, detailed procedures and due diligence on cybersecurity go a long way to lessen risks from third parties but cannot defend against all cyberthreats," Pascale says. "It is vital that co-ops remain cyber alert throughout all third-party contracts."

NRECA offers several resources to aid co-ops in making their contracts more cybersecure at cooperative.com/cybersecurity.

MEET OUR TEAM

Carter Manucy
Director, Cybersecurity
Carter.Manucy@nreca.coop

Ryan Newlon
Cybersecurity Principal
Ryan.Newlon@nreca.coop



Justin Luebbert
Cybersecurity Principal
Justin.Luebbert@nreca.coop

Meredith Miller
Data Scientist Principal
Meredith.Miller@nreca.coop

CONTACT US AT: membersecurity@nreca.coop

NRECA CYBERSECURITY RESOURCES FOR CO-OPS

NRECA RESEARCH

NRECA Research complements the resources and services provided by NRECA to address the needs of electric cooperatives. Through NRECA Research, our members can leverage extensive internal expertise and established industry partnerships to develop and demonstrate new technical capabilities that directly address challenges and opportunities of the future electric grid.

www.cooperative.com/programs-services/bts/research/Pages/default.aspx

KEY CYBERSECURITY PAGES ON COOPERATIVE.COM

Cybersecurity Overview and Key NRECA Contacts
www.cooperative.com/topics/cybersecurity/Pages/Cybersecurity-Overview-and-Key-Contacts.aspx

Featured Cybersecurity Resources, Fact Sheets and News
www.cooperative.com/topics/cybersecurity/Pages/default.aspx

TOOLS AND GUIDES

Co-op Cyber Goals Program
www.cooperative.com/programs-services/bts/rc3/cyber-goals/Pages/default.aspx

Cybersecurity Self-Assessment
www.cooperative.com/programs-services/bts/Pages/Assessing-Your-Cybersecurity-Posture.aspx

Cybersecurity Tabletop Exercise Toolkit
www.cooperative.com/programs-services/bts/rc3/Pages/RC3-Cybersecurity-Tabletop-Exercise-Toolkit.aspx

Co-op Cybersecurity Lexicon
www.cooperative.com/programs-services/communications/toolkits-and-samples/Pages/Secure/Co-op-Cybersecurity-Lexicon.aspx

Reputation Management and Cybersecurity Crisis Communications
www.cooperative.com/programs-services/communications/toolkits-and-samples/Pages/Secure/Reputation-Management-and-Crisis-Communications.aspx

Cybersecurity Guidebook Series
www.cooperative.com/programs-services/bts/rc3/Pages/RC3-Cybersecurity-Guidebook-Series.aspx

Advisory: Managing Your MSP Vendor for Cybersecurity
www.cooperative.com/programs-services/bts/rc3/Pages/Managing-MSP-for-Cybersecurity.aspx

Advisory Series: Cybersecurity Information Sharing
www.cooperative.com/programs-services/bts/rc3/Pages/Cybersecurity-Information-Sharing.aspx

Infrastructure Resource Hub and Federal Funding
www.cooperative.com/infrastructure

THREAT ANALYSIS AND REPORTING

NRECA Threat Analysis Center
www.cooperative.com/programs-services/bts/research/Pages/Threat-Analysis-Center.aspx

Cyber Incident Response Plan Development Workshop
www.cooperative.com/conferences-education/web-based-learning/Cyber-Incident-Response-Plan-Development-Workshop/Pages/default.aspx

Join Us For Engagement And Learning

Cybersecurity Update Webinar Series
www.cooperative.com/conferences-education/web-based-learning/cybersecurity-update-webinar-series/Pages/default.aspx

Co-op Cyber Tech Conference
www.cooperative.com/conferences-education/meetings/Co-op-Cyber-Tech/Pages/default.aspx

ICS-REC: Industrial Control Systems for Rural Electric Cooperatives
www.cooperative.com/programs-services/bts/research/ics-rec/Pages/default.aspx

Cybersecurity Member Advisory Group (CSMAG)
www.cooperative.com/programs-services/bts/cybersecurity/Pages/default.aspx

For more information and updates, visit www.cooperative.com/topics/cybersecurity