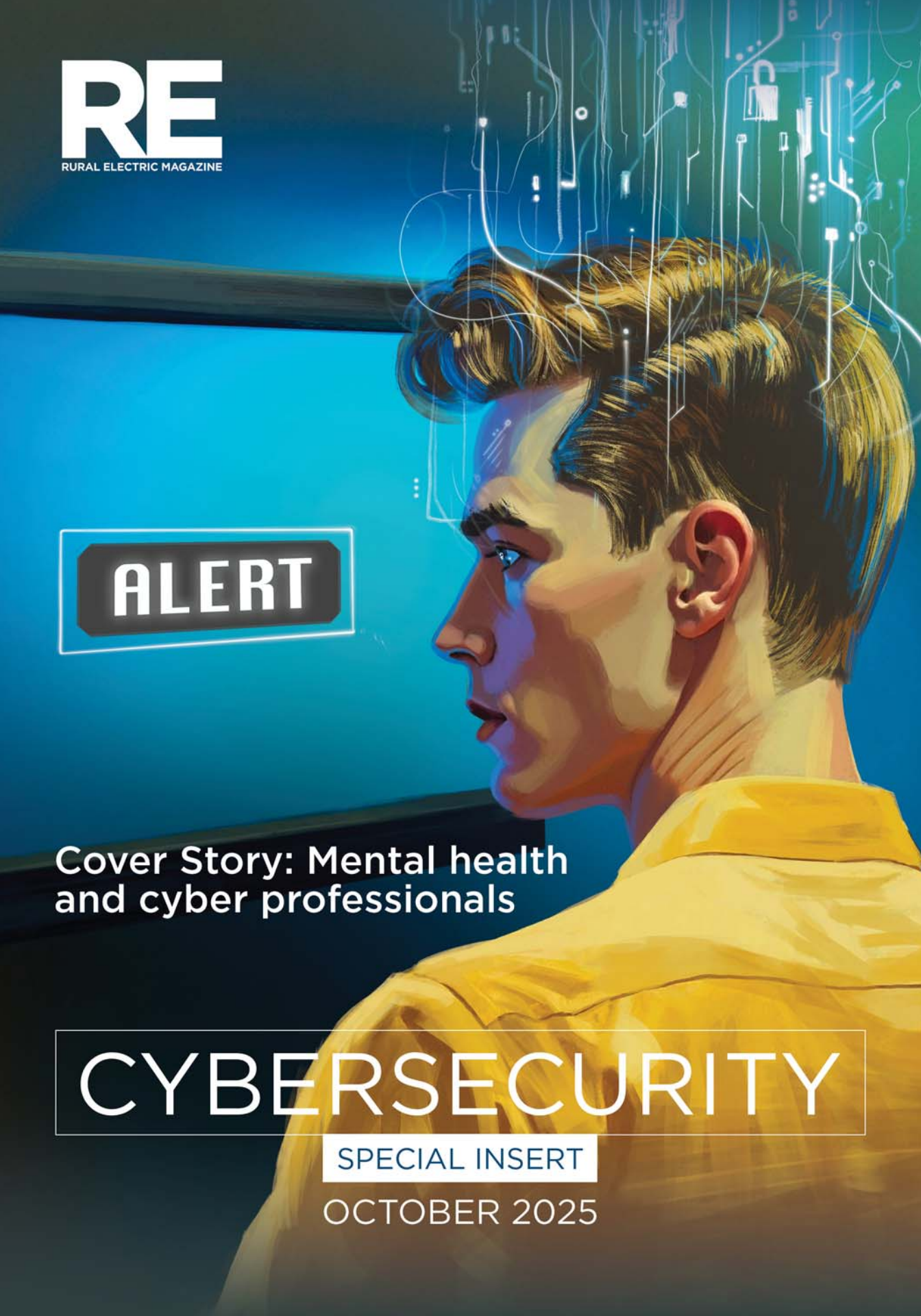
RE
RURAL ELECTRIC MAGAZINE



Cover Story: Mental health and cyber professionals

CYBERSECURITY

SPECIAL INSERT

OCTOBER 2025

WELCOME TO THE SPECIAL CYBERSECURITY INSERT

TABLE OF CONTENTS

Cover Story: Pressure Cooker | **2**
Feature: Finding Rural Cybersecurity Professionals | **7**
Feature: Cyber Risk as Business Risk | **11**
Feature: How Mature Is Your Co-op's Cybersecurity? | **14**
Feature: Improving IT Communication | **15**
Resources, Opportunities and Contacts | **16**

Advertorial/Sponsor Content
Bastazo | **4**
DeNexus | **8**
Insane Cyber | **12**

Cover Illustration By: Jerry Mosemak/NRECA

PRESSURE COOKER

Cyber professionals are managing unprecedented mental health challenges

By Scot Hoffman

Angela Hare saw something very different about the way electric cooperative leaders in western North Carolina managed their crews amid the devastation and prolonged outages caused by Hurricane Helene in late 2024.

"They flipped the script," says Hare, vice president for information technology, member services and metering at Central EMC in Sanford, North Carolina.

She describes how some co-op managers there, knowing the relentless recovery work would likely go on for weeks, set up a system for crewmembers to be able to go home and recover, physically and mentally, one day per week until the restoration was complete.

"I'd never seen that before in our state, and we get a lot of hurricanes," she says. "With co-ops, what's ingrained in us is, 'Get the lights on, get the lights on, get the lights on.' That's what we do. And that propagates into every aspect of a co-op."

This new focus is part of an encouraging trend Hare says she's seeing among co-ops in her state to acknowledge and prioritize the role mental health plays in an industry where nearly all facets have become excessively demanding, intense and change-driven. And as an IT professional, she says, there's no sector more in need of this type of shift than the cybersecurity field.

"Stress in cyber is real," Hare says. "It's like preparing for a hurricane you can't see, and doing it every single day. As leaders, we must pay attention to our employees' 'burnout gauge' before it's too late."

Numbers from recent studies support the idea that there is a worsening "burnout epidemic" among frontline employees.

A 2024 study conducted by Censuswide and commissioned by the global cyber performance center Hack the Box found that 84% of cyber-security professionals reported feeling burnout that was harming their job performance. Respondents cited factors like intense workload and "alert fatigue" from an explosion of new cyberthreats, staffing shortages, and a lack of recognition and support from leadership as the primary causes.

The psychological impacts, the study noted, are leading to rampant increases in absenteeism, lost productivity, career switching, persistent anxiety, substance abuse, sleep issues and even symptoms akin to PTSD.

Patrick Kelley, CEO of Critical Path Security, travels more than 40 weeks a year giving talks to IT and cybersecurity professionals. Until recently, those sessions were nearly all technical in nature, explaining tools and system for using AI or building a more secure network.

Lately that's changed.

"Almost every talk I do now is about mental health," he said. "People are really ready to hear this message."

continued on page 6

Illustration By: Jerry Mosemak/NRECA

In electric utilities, compliance is mandatory—but it doesn't always equal security. Relying on CVSS scores alone may pass audits but let critical risks slip through. True resilience means taking a risk-based approach that meets compliance requirements and reduces real-world threats, prioritizing vulnerabilities by actual risk to your unique systems.

The Limits of the Compliance-First Mentality

Compliance requirements like NERC CIP-007 help enforce minimum standards, but too often, teams focus on tracking whether something was done, rather than why it was done. The result? Patching decisions driven by policy timelines, not operational risk.

Let's face it: patching everything isn't feasible or desirable. Every patch carries risk—from unplanned downtime to compatibility issues. But not patching at all can put you at more risk.

That's where context becomes critical. Teams need to weigh operational impact against threat likelihood, moving away from blanket patching and toward targeted mitigation.

Why CVSS Isn't Enough

The Common Vulnerability Scoring System (CVSS) is the industry standard for measuring severity. Teams using this scoring may think they are enacting "risk-based" management, but severity isn't the whole story.

A CVSS Base Score doesn't consider whether a vulnerability is exposed in your environment. A 9.8 might be safely tucked behind protection in your system, while a 5.4 could be sitting wide open on a critical asset.

CVSS can accommodate an environmental score, but it requires manual input and deep system knowledge. Most teams don't have time to customize scores for every vulnerability on every asset. Instead, they default to the base score, even while knowing its limitations.

In fact, 12% of vulnerabilities listed in the CISA KEV Known Exploited Vulnerabilities (KEV) catalog are rated as medium or low. Most organizations aren't even able to handle all vulnerabilities with a Critical severity for their assets.

But not all critical vulnerabilities will be exploited. And not all medium or low vulnerabilities pose little risk. Attackers don't care about your CVSS threshold. They care about what gets them access.

By focusing on CVSS severity alone, teams are doing more work than they need to, while still not doing the work they should do.

Example

CVE-2024-37085 [Base CVSS Score and Severity: 6.8 (MEDIUM)]

This CVE likely would not have been a high priority when released based solely on its CVSS score. The dual requirements of user interaction and a high degree of necessary privileges contributed to its Medium severity. However, misconfigured ESXI servers presented an open target, and this CVE was quickly used in ransomware campaigns to gain persistence after an initial compromise.

A Better Framework: SSVC

If your organization is only prioritizing CVEs based on their CVSS scores, it's time to raise the bar. At a minimum, you should be actively tracking and remediating vulnerabilities listed in the CISA KEV catalog—these are proven threats, not just theoretical risks. But to truly adopt a risk-based approach, you need to go further.

The Stakeholder-Specific Vulnerability Categorization (SSVC) methodology provides a structured way to decide what matters most to you.

Instead of just asking, "How bad is this vulnerability?" SSVC asks:

- Is it exploitable?
- What is the system exposure?
- How critical is the vulnerable system?
- Could it impact safety or mission?

It takes into account both technical and organizational risk. Based on those factors, vulnerabilities are assigned one of four priorities:

Defer – Low urgency, low exposure

Scheduled – Routine patching needed

Out-of-Cycle – Requires immediate attention outside regular schedule

Immediate – Highest priority, urgent mitigation

SSVC is powerful for utilities because it relies on relatively static data like asset criticality, system exposure and safety controls (making it scalable), while layering in dynamic factors like exploitability to provide a realistic snapshot of impact, all without requiring advanced cybersecurity expertise.

Better yet, it gives you a repeatable, explainable reason for every decision. That's gold during an audit.

How Bastazo Can Accelerate Your Move to Risk-Based Cybersecurity

Compliance is the floor, not the ceiling. With SSVC and risk-based vulnerability management, you can move from reactive patching to proactive defense.

Bastazo can help your team by automating SSVC logic, but also by incorporating adversary intelligence—bringing the 5% of vulnerabilities that truly matter to the surface.

- Automatically prioritize vulnerabilities on your assets using SSVC
- Notifications when decision points change (ex: when an exploit is released)
- Simplify reporting of decision justification for audits or internal use

Want to see how it works? You can do it yourself and get a taste of SSVC's impact with our free SSVC Categorization Worksheet here:

Bastazo.com/SSVC-Tool

Or reach out to schedule a demo of Bastazo's full AI-informed prioritization and remediation platform. ■

continued from page 3

Kelley, a 30-year IT security professional, pairs his work experience with his personal story of managing PTSD in his mental health talks. He likens modern cyber work to a pressure cooker without a relief valve.

"When you hear the whistle on a pressure pot, you know everything's okay, good things are happening," he says. "But what happens if you take that valve away? It becomes a bomb."

Kelley says IT and cyber workers are susceptible to blaming themselves and thinking it's their responsibility for "unburning out" themselves. He encourages cyber pros to lean on their colleagues in the program the way operations crews do during outages and mutual aid events.

"The way that we move forward is to be more like the linemen in those trucks," he says. "We need to support each other like they do."

He offers five pieces of advice for cyber professionals to cope with the strain of their career: time off, journaling, meditation, social support and professional help.

Improving mental health "takes time and perseverance," he says. "You have to be patient with yourself."

The broader cybersecurity industry is beginning to respond with changes that embed mental health into cyber-resilience strategies, including embracing more flexible work arrangements, implementing post-incident wellbeing checks and instituting leadership training that destigmatizes mental health discussions.

Rachel Price, NRECA's learning and development manager, says her team has been adding resilience, mindfulness and stress management to many of the association's trainings and development opportunities.

"For the individual, for a leader, a manager, an organization, how can they recognize that their employees are under stress," she says. "And it's about encouraging conversations, listening and hearing what [employees] are trying to say before it gets to the burnout point."

Price adds that a critical bulwark against burnout is a familiar co-op principal: community.

"It's about finding your people," she says. "You need people for all different things. You need them for when you're overwhelmed with your workload. You need them for empathy, for problem-solving, for perspective."

She encourages co-ops to offer trainings, events and workshops that bring cyber professionals together with other staff to help them develop a cohort of support.

"Development programs at NRECA have a huge community aspect to them," she says. "We have the bigger workshops, but we also have mentoring and peer coaching, where you have a smaller team of maybe five or six people to talk about the challenges that they have and get different perspectives."

For Hare, who's been at Central EMC for more than 25 years, her hope is that the emotional awareness shown in the co-ops' operational response to Hurricane Helene will find its way throughout the program, especially to IT and cybersecurity teams.

"My hat is really off to those CEOs. … They set a new standard," she says. "I hope we continue that." RE

> "Stress in cyber is real. It's like preparing for a hurricane you can't see, and doing it every single day. As leaders, we must pay attention to our employees' 'burnout gauge' before it's too late."
>
> —Angela Hare, Vice President for Information Technology, Central EMC

Chris Jones, president and CEO of Middle Tennessee Electric, testifies before the House Homeland Security Committee on steps electric co-ops are taking to attract cyber professionals to their rural communities.

Photo By: Denny Gainer/NRECA

'A LITTLE MORE NIMBLE'

Co-ops use innovation to fight a shortage of rural cyber talent

By Scot Hoffman

Josef Chesney has what he calls a "moonshot" idea for mitigating the worsening cybersecurity staffing challenges in rural America: start a Cybersecurity Service Corps modeled on the National Health Service Corps created in the 1970s to bring doctors and nurses to rural areas.

"It would take a lot of effort, but I think there's potential here," says Chesney, the cybersecurity program manager at Powder River Energy (PRECorp) in Wyoming. "Get these kids into cybersecurity programs, get their education paid, then they spend four years in a rural community."

He says the broader impact of such an initiative could be opening the eyes of young professionals to the allure of rural living and electric cooperative culture.

"You know what happens after four years of living in a rural community? You might like it. You might want to stay. You might go, 'Wow.' That's what happened to me."

Over the past decade or so, a major gap has opened in the availability of cyber talent in urban areas versus rural ones. The perception of limited amenities, lower salaries and fewer advancement opportunities in small towns are among the primary factors.

And the trend has been exacerbated by an explosion of online threats and a worrying attrition rate among cyber professionals, who are experiencing burnout at alarming levels. The cyber talent shortage in the U.S. alone is around 225,000.

Chesney admits his moonshot idea of a national Cyber Corps is not likely to happen any time soon, but he says electric cooperatives

continued on page 10

Cyber Risk in Electricity Transmission and Distribution: A Call for Proactive Risk Management

DENEXUS™

Escalating Threat: The Impact of Macro Trends on Cyber-Physical Infrastructure

Across North America, a convergence of macro trends is intensifying cybersecurity risk, particularly for cyber-physical critical infrastructure like the electric grid. Rapid digitalization, increased connectivity of operational technology (OT) systems and more sophisticated threat actors have expanded utilities' and co-ops' attack surfaces. Simultaneously, aging infrastructure, grid decentralization and geopolitical tensions are straining system reliability.

The shift toward distributed energy resources and real-time control introduces new vulnerabilities faster than utilities can address them. Many electric cooperatives—especially in rural areas—operate with limited budgets and staff, making them attractive targets for malicious actors seeking disruption or financial gain.

Understanding Cyber-Physical System Risk

The sector increasingly relies on cyber-physical systems—technologies that link digital controls with physical assets like transformers, switches and circuit breakers. While essential, this convergence introduces significant risks. OT outages can lead to real-world consequences: environmental harm, safety hazards, equipment damage and blackouts.

Operational design compounds the issue. Planned outages occur every 3 to 5 years, and system upgrades follow multi-year cycles, leaving vulnerabilities unaddressed for extended periods. Much infrastructure includes end-of-life components with known flaws, unprotected remote access points and a shortage of cybersecurity specialists. About half of these systems use proprietary protocols and software, making conventional cybersecurity tools inadequate.

Challenges for Stakeholders

While the risk is understood, translating it into financial and operational decisions remains a major challenge. CISOs struggle to convey risk in business terms. CFOs and risk managers lack visibility to prioritize cybersecurity investments. Insurance teams are often unsure whether current policies cover actual exposures—especially events causing physical damage.

This disconnect leads to underinvestment and under-preparedness. Most cyber insurance policies exclude physical damage, while property insurance often excludes cyber triggers. Without solid data and analytics on OT cyber loss events, planning and transferring risk remains speculative.

A Framework for Cyber-Physical Risk Management

Effective cyber risk management requires a holistic, risk-based approach:

1. **Understanding the Risk:** Collect and analyze data to assess threat likelihood and impact.
2. **Avoidance:** Eliminate vulnerabilities through architectural redesign or cyber-informed engineering.
3. **Mitigation:** Apply hardening, segmentation, or access controls when feasible and cost-effective.
4. **Transfer:** Shift long-tail risk to insurers using policies that cover physical damage from cyber events with appropriate limits.
5. **Acceptance:** Acknowledge and monitor residual risk that cannot be addressed through other means.

This framework balances technical defense with financial responsibility, enabling boards and executives to make informed decisions.

Why Data Is the Cornerstone

Cyber-physical risk management hinges on accurate and timely OT data. This data must support operational decisions, financial planning and insurance discussions. OT-specific cyber risk quantification platforms are essential.

DeRISK™ by DeNexus is one such platform, built for OT environments. It integrates internal telemetry, external threat intelligence and proprietary analytics based on frameworks like MITRE ATT&CK. DeRISK simulates attack paths, loss scenarios and mitigation outcomes, enabling dynamic and data-driven risk management.

Tailored for Electricity T&D Systems

DeRISK™ is customized for electric transmission and distribution. It ingests utility-specific inputs—such as substation diagrams, transformer ratings and toll prices—to model cascading effects from cyber incidents. Outputs include estimated revenue loss, equipment damage, regulatory fines and environmental penalties.

This specificity is crucial for under-resourced co-ops. Rather than relying on generic models, they gain actionable insights aligned with their unique infrastructure and geography.

Cyber-physical risk models must also account for cascading failures in interconnected T&D networks. A breach at one substation or control point can propagate rapidly, affecting both digital and physical assets across a region. These failures may cause voltage instability, equipment overload or widespread blackouts. Traditional models often assess systems in isolation, but effective OT risk models must simulate these network-wide impacts. This ICS/OT/SCADA-aware approach is vital for prioritization, resource allocation, and resilience planning.

Solving the Full Risk Management Puzzle

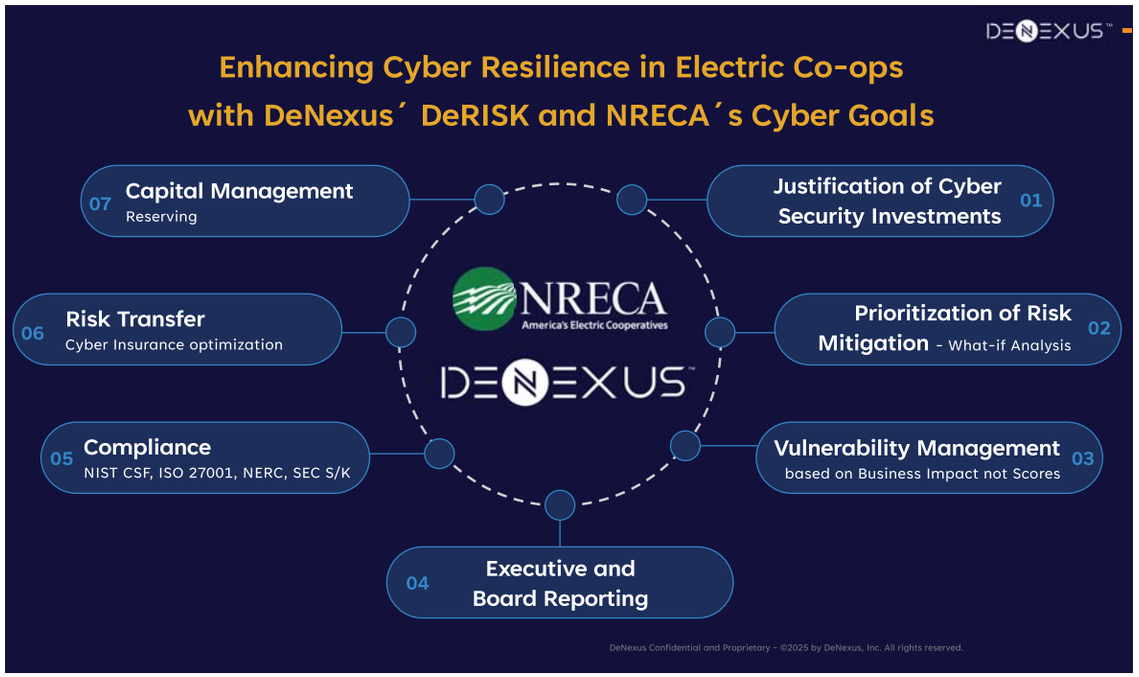
With accurate OT data and analytics, organizations can address all aspects of cyber risk—from compliance and capital planning to insurance and executive reporting. DeRISK™ helps shift cybersecurity from a technical concern to a strategic advantage.

Meeting the Needs of Every Stakeholder

Robust OT data not only improves technical outcomes but also aligns the priorities of CISOs, CFOs and insurers. CISOs can demonstrate ROI; CFOs can assess capital needs; insurance teams can negotiate more tailored policies. For co-ops and grid operators with tight budgets, this unified, data-driven approach enables better decision-making and clearer prioritization.

Conclusion

Cyber risk to the electric grid is no longer theoretical—it's a present and growing challenge, particularly for co-ops and small utilities. By embracing a risk-based strategy supported by OT-specific data and tools like DeRISK™, these organizations can move beyond compliance to proactively safeguard operations, finances, and public trust. ■



continued from page 7

Chesney

Oursler

have two unique advantages for attracting candidates: co-op culture and flexibility.

"We're not going to be able to pay you the highest pay, but you're going to have good benefits—medical, retirement—a good place to raise your family, the ability to innovate," he says. "And we're small, but sometimes small is good. We can be a little more nimble. If you show the talent and the ability and the desire, we can make changes, and we can get you to where you want to be."

Cole Oursler, director of information services at Mountain View Electric in Colorado, says managers need to be patient and creative in finding new IT/cyber talent.

"We're not like the giant IOUs. We'll never be able to pay what they pay," he says. "The way we respond is to be innovative in our solutions."

Oursler, who also chairs NRECA's Cyber Member Advisory Group, notes that starting a cross-training program that exposes internal employees to various tasks will help create a more versatile workforce and can ease the strain of having empty chairs on the cybersecurity team.

Looking at candidates that may not fit the classic training and background of a cyber professional, he adds, can bring new viewpoints, creativity and innovation to the team, key attributes when you're trying to stay ahead of cyber criminals.

"Sometimes we don't really need what we think we need," says Oursler. "If I find the right type of candidate, I can train them to do the technical stuff.

Chris Jones, president and CEO of Middle Tennessee Electric, also sees developing local talent as a key part of the solution.

"Many rural regions lack institutions that offer advanced cybersecurity courses," he told a hearing of the House Homeland Security Committee earlier this year. To address this, "co-ops are increasingly focused on … partnerships with educational institutions."

He noted that the recently introduced Cyber PIVOTT Act would expand cybersecurity internship opportunities to electric co-ops in rural communities.

"Developing a talent pipeline with off-ramps into rural communities will help grow a local, skilled cybersecurity workforce to protect critical infrastructure in these communities," he said. "Initiatives like those in the Cyber PIVOTT Act bring much-needed focus to the cyber workforce needs of rural America. … Co-ops and our rural communities have a lot to offer in protecting America's critical infrastructure measures." RE

> "You're going to have good benefits—medical, retirement—a good place to raise your family, the ability to innovate. And we're small, but sometimes small is good. We can be a little more nimble."
>
> —Josef Chesney, Cybersecurity Program Manager, Powder River Energy

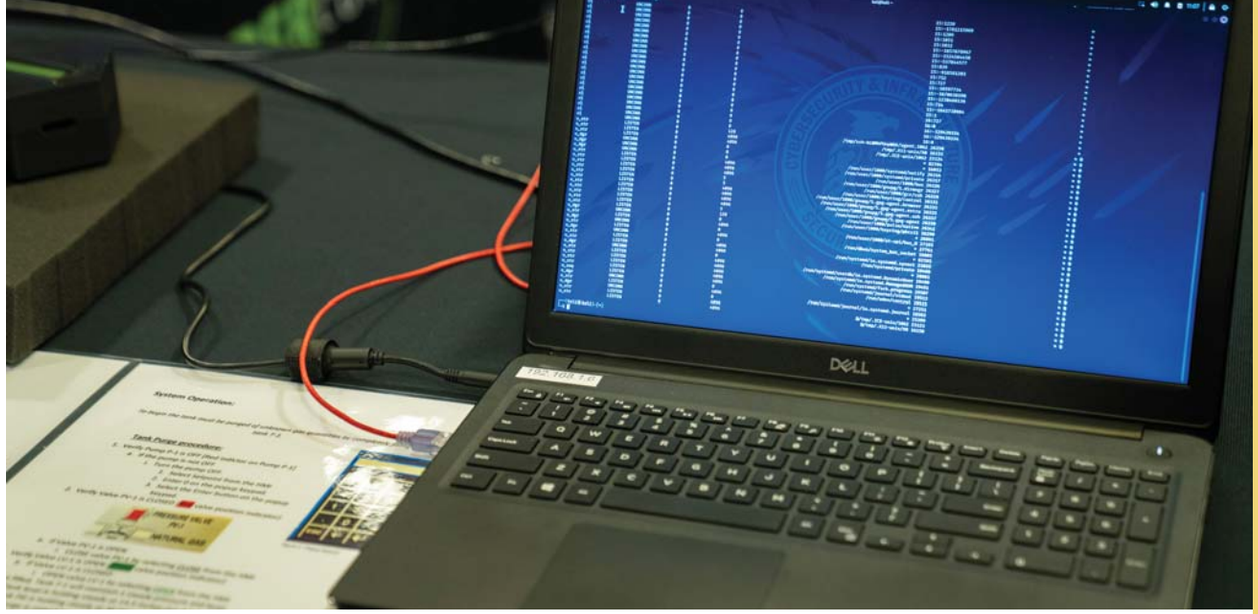


Photo By: Denny Gainer/NRECA

UNDERSTANDING CYBER RISK AS BUSINESS RISK

By Cathy Cash

"What does this mean in real dollars?" It's a question Adrian McNamara hears a lot.

With rapid increases in internet-connected IT and OT systems and an explosion in the number and sophistication of global cybersecurity threats, the task of helping electric cooperative leadership and board members get their arms around what's exactly at stake and what to prioritize is becoming more and more complex.

"We have a lot of risk out there … and we can't always quantify it,'" says McNamara, NRECA's cybersecurity program manager. "You want to be able to say to your board, 'Here's what we're doing. Here's what we need to be doing more of. Here's where we need to invest.'"

He says keeping open lines of communication with leadership and the board on the latest threats, preemptive measures and cybersecurity needs is essential. But there's one tactic that truly cuts through the complexity: "Putting a dollar figure on it."

"Even when you're implementing proper cybersecurity controls, your co-op is still at risk," he says. "To take the next step, you need to quantify your cyber risks as financial risks."

To help facilitate that, NRECA launched a pilot program that can take real-time information regarding IT and OT systems as well as cyber risk mitigation steps and generate an analysis that quantifies cyber vulnerability and assigns a dollar amount to the overall risk. Begun in March, the Cyber Risk Quantification Pilot Program is free for participating co-ops and leverages the DeRISK Quantified Vulnerability Management platform from DeNexus.

"By putting a dollar amount on cyber risk, co-ops can maximize their investment in critical cybersecurity defenses to protect their systems." McNamara says.

For example, the platform may assess a co-op as having a $1 million cyber risk exposure. That number may fall by as much as $250,000 if the co-op reports that it has completed NRECA's 20 Co-op Cyber Goals.

"This will help provide co-ops with benchmarks and risk exposure to help IT and OT managers explain the value of cybersecurity investments to offset the view of cybersecurity as a pure cost center," says NRECA Cybersecurity Director Carter Manucy.

Co-ops interested in joining the pilot, which runs through early 2026, can contact McNamara at Adrian.McNamara@nreca.coop. RE

Insane Cyber™

Dark Corners of the Substation

The OT Assets You've Forgotten to Protect

BY DAN GUNTER,
CEO and Founder, Insane Cyber

When most electric co-operatives think about OT cybersecurity, the focus naturally drifts to the big, visible pieces of the puzzle: the SCADA master, the firewall, the front-end historian. But in the quieter corners of substations, field sites and pole-top cabinets lie the assets that are often overlooked and increasingly targeted.

These "dark corners" of the OT environment, like legacy RTUs, unmanaged switches, engineering workstations, serial converters and even forgotten cellular modems may not show up on a network map or asset inventory, but they can pose real risks. And for co-ops with limited teams and budget, securing them can feel like a daunting task.

> "It doesn't take a major audit or heavy lift to start shining a light into these gaps."

Here's the good news: it doesn't take a major audit or heavy lift to start shining a light into these gaps. With the right host and network-level monitoring tools, even small teams can gain visibility, detect risk, and act before something goes wrong.

The Forgotten Layers of the Substation Stack

Most co-ops have worked to harden the obvious endpoints like primary SCADA servers and external-facing firewalls. But deeper inside the control environment, the picture tends to get fuzzier:

- **Engineering laptops used for maintenance** might still have unpatched software or saved credentials.
- **Unmanaged switches** often don't log traffic or support access control, making lateral movement easy if compromised.
- **Out-of-band access paths**, like backup cellular or serial modems, are often left connected—and unmonitored.
- **Legacy field devices** may still run insecure protocols like DNP3 or Modbus with no authentication or encryption.

What's more, many of these devices weren't designed with cybersecurity in mind. They're stable, they "just work"—and that's part of the problem. In the absence of visibility, a silent compromise can persist for months.

Why Small Teams Need Smart Visibility

For small and mid-sized co-ops, conducting full-blown cybersecurity audits across all remote sites isn't always realistic. But the goal isn't perfection—it's progress.

That's where lightweight host and network monitoring solutions come in. Rather than requiring intrusive installs or expensive integrations, modern tools can plug into a network tap or span port, passively observe traffic, and flag suspicious behavior.

Some solutions can also collect logs and system data from host devices, like substations' HMI workstations or relay configuration laptops, without interrupting operations. This gives analysts context: what software is running, when configurations change and what devices are talking to each other.

Together, host and network visibility can uncover things like:

- Unauthorized firmware changes or device reboots
- Lateral movement across switch ports
- Unauthorized outbound traffic from substation devices
- Unexpected use of USB storage or configuration tools

This kind of early detection allows small teams to focus on anomalies that matter, instead of digging through syslogs or relying on a phone call when "something looks weird."

A Pragmatic Approach: Shine a Flashlight, Don't Build a Lighthouse

Improving OT security doesn't mean hiring a dozen new analysts or launching a yearlong compliance project. Sometimes it's as simple as getting eyes on what you already have.

In rural co-ops and large utilities alike, and one thing is consistent: You can't protect what you can't see. Today's emerging OT cybersecurity tools are designed to help discover what's hiding in plain sight that traditional network monitoring tools can't uncover.

Start with the Known Unknowns

If you're wondering where to start, here's a practical checklist:

- ❒ **Inventory your field assets, especially unmanaged or legacy devices.**
- ❒ **Check for persistent out-of-band connections like dial-up, cellular, or USB.**
- ❒ **Deploy passive monitoring at a few critical substations to capture baseline traffic.**
- ❒ **Monitor engineering laptops or field workstations for software changes or suspicious activity.**
- ❒ **Correlate host and network activity to catch subtle threats.**

See the Shadows Before They Become Incidents

In today's threat landscape, it's not always the obvious targets that attackers go after. Sometimes, the easiest way into a system is through the assets no one's watching.

Electric co-ops, especially those with lean teams and broad geographic footprints, need tools that match their reality. By deploying host and network visibility where it counts most—in those forgotten corners—you can uncover risks early, prioritize remediation, and protect your members without breaking the bank.

It's not about catching everything; it's about not being caught off guard. ■

HOW MATURE IS YOUR CO-OP'S CYBERSECURITY?

By Cathy Cash

When it comes to cybersecurity, there's a temptation to assume that larger electric cooperatives have more effective or comprehensive programs.

In fact, says Justin Luebbert, NRECA's senior manager of cybersecurity, the number of members, employees, meters and poles a co-op has is not necessarily predictive of a strong cyber defense. He says factors related to "cyber maturity"—how seriously cybersecurity is regarded by leadership, strong governance and a cyber-aware culture—are far more determinative of cyber strength.

"While organizational size may suggest access to more resources, it doesn't guarantee those resources are used effectively," says Luebbert. "Cybersecurity maturity reflects how well an organization applies its tools, processes and people to manage risk."

Large co-ops, he says, may have dedicated cyber teams but lack cross-functional coordination to cover their expansive infrastructure and attack surface. Small or mid-sized co-ops may be skilled and able to communicate easily across functions but have a modest budget for cyber training or equipment.

NRECA's Project Guardian—launched in 2024 under a $4 million agreement with the Department of Energy to help rural and municipal utilities strengthen their cyber posture—recently introduced its Categorization of Cybersecurity Maturity for Cooperatives tool. It helps co-ops identify where they are today and provides a roadmap for where to go next to build a stronger, more sustainable defense.

"Aligning cybersecurity resources to an organization's maturity level—not just its size—is critical for effectiveness," says Luebbert.

For a utility categorized as "Initial" in the maturity framework—with limited staff, no dedicated budget and minimal training—a 15-page incident response template may be too complex to execute during a crisis, whereas, a concise, three-page plan with clear roles and actionable steps may be more effective.

> "Aligning cybersecurity resources to an organization's maturity level—not just its size—is critical for effectiveness."
>
> —Justin Luebbert, Senior Manager of Cybersecurity, NRECA

"It's about making resilience achievable, no matter the size," Luebbert says. "Project Guardian's categorization tool empowers cooperatives to align cybersecurity with actual capability—not just budgets or headcounts."

Project Guardian works with DOE's Rural and Municipal Utility Advanced Cybersecurity Grant and Technical Assistance Program and Office of Cybersecurity, Energy Security and Emergency Response. It runs through April 2029. RE

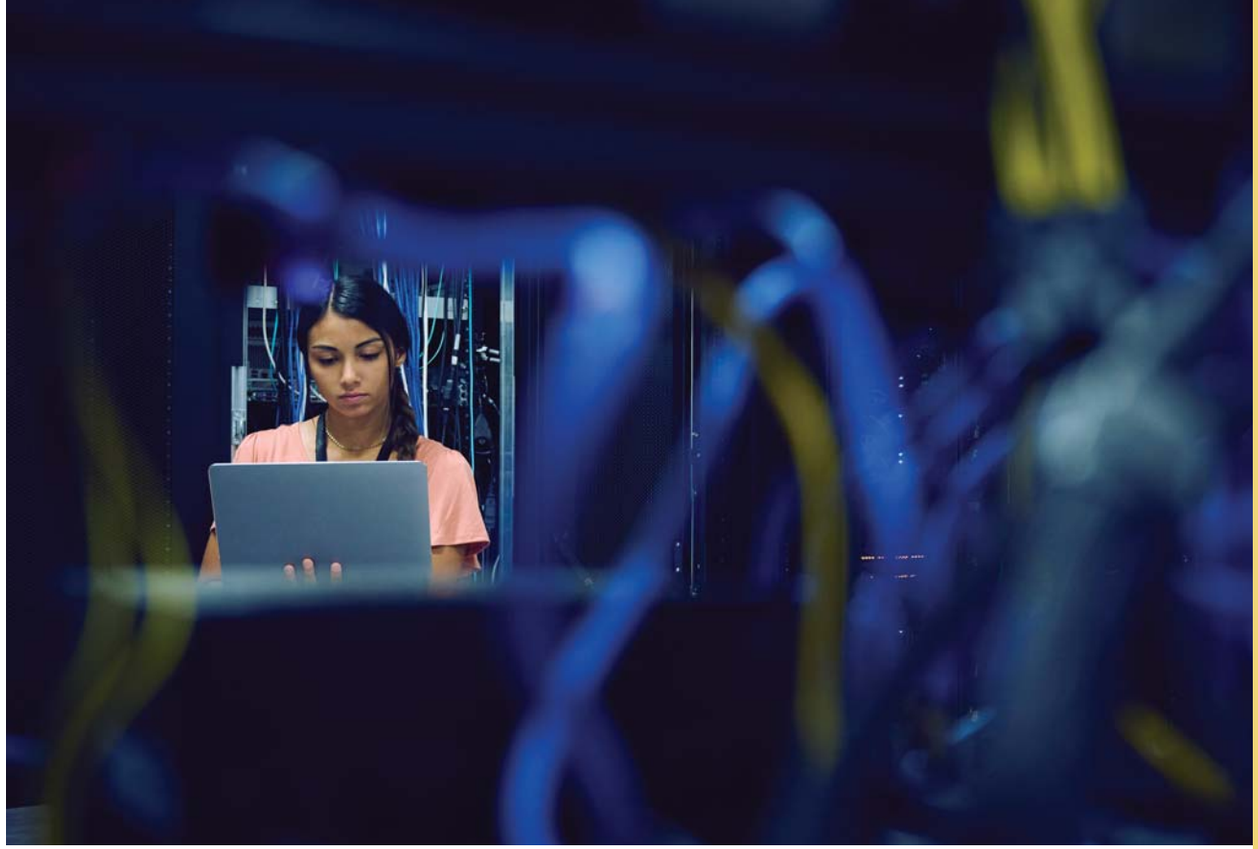


Photo By: Tetra Images/Getty Images

IMPROVING IT COMMUNICATION

By Cathy Cash

When Anthony Kent left big tech for Four County EMC, he learned that to communicate effectively with co-op leaders, he had to get out of the weeds of information technology and speak their language.

"It's on us to be better communicators and help leadership understand what we are talking about," says Kent, IT vice president at the Burgaw, North Carolina-based co-op. "We IT people need to learn to communicate better with leadership so they want to communicate with us."

Tanner Greer, senior vice president and chief technology officer at Lenior-based Blue Ridge Energy, says, "Boards understand strategic plans, and that's what they want to be presented with."

He recommended planning no more than three years out to keep pace with technology changes.

"Formulate initiatives. Create metrics to show it's getting done and ways to track progress."

CEOs want to see tech proposals that show a project's financial impact and risks and how it affects members and employees.

Any IT strategic plan "needs to focus on these top three," Greer says. "And never think that because you explained it once that it's understood."

Kent and Greer offer several tips for how IT staff should approach discussions about tech projects, challenges and system requirements to CEOs and board members:

- Keep jargon and acronyms to a minimum.
- Break down complex technical information.
- Put yourself in their shoes.
- Keep to an appropriate level of detail.

IT solutions should address business goals and be communicated as such, Kent says. Finding cross-functional collaboration and support wherever possible will help boost their success.

"Know that IT is more than a support function. We are business enablers," Kent says. "We touch everyone." RE

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

Project Guardian
www.cooperative.com/programs-services/bts/research/project-guardian/Pages/default.aspx

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

Co-op Mutual Assistance Program
https://www.cooperative.com/topics/cybersecurity/Pages/Cyber-Mutual-Assistance-Program.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

Engagement and Learning Opportunities

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

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

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

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

OUR TEAM

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

Justin Luebbert
Cybersecurity Senior Manager
Justin.Luebbert@nreca.coop

Ryan Newlon
Cybersecurity Principal
Ryan.Newlon@nreca.coop

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

Adrian McNamara
Cybersecurity Program Manager
Adrian.McNamara@nreca.coop

FOR MORE INFORMATION AND UPDATES, VISIT WWW.COOPERATIVE.COM/TOPICS/CYBERSECURITY

Co-op
Cyber Tech

SAVE THE DATE

2026 Co-op Cyber Tech

June 3-5, 2026

JW Marriott
Downtown Indianapolis
Indianapolis, Indiana

Scan for details.

NRECA
America's Electric Cooperatives

Learn more at **cooperative.com/co-opcybertechstd26.**