BENS INSIGHTS:
Elevating Thought Leadership in National Security

BUSINESS EXECUTIVES FOR NATIONAL SECURITY
SECURING AMERICA'S FUTURE

Securing the U.S. Electric Grid: How Are We Meeting the Challenge?

March 2025

Securing the U.S. Electric Grid: How Are We Meeting the Challenge?

The U.S. electric grid is a vital element of the U.S. economy, national security, and the way of life of the American people. It is also under increasing threat from hostile states, terrorist and criminal organizations, and extreme weather events. The number of physical attacks on the grid have increased in recent years, and last year, 42% of critical infrastructure companies, including those in the energy sector, suffered data breaches from cyberattacks.

To better understand the threats facing the grid and ongoing efforts to address them, BENS interviewed four industry experts with experience addressing different aspects of the electric grid and its security, including owner-operators of grid assets, and experts on cybersecurity and disaster resilience and recovery: **David Velazquez**, President and CEO of PECO, an Exelon utility; **Jay Owen**, President of Schneider Electric Federal; **Rafael Sosa**, of Sosa & Arvelo; and **Ben Trowbridge**, Regional Transmission Organization Board member and cybersecurity advisor.

David Velazquez
President and CEO of PECO

Jay Owen
President of Schneider Electric Federal

Rafael Sosa
Sosa & Arvelo LLC

Ben Trowbridge
Regional Transmission Organization Board

Note: Interviews have been edited for length and clarity. The views expressed are their own and may not reflect those of their employers or BENS.

We are seeing a trend of year-on-year increases in the number of attacks on the grid. What are the threats, or combination of threats to grid assets that most concern you?

David Velazquez: For any utility—the Exelon utilities included— safety and reliability are forefront of our minds every day we come into work. When you think about the history of utilities, that has been our mission for 100 years. It's all about safety and reliability.

I put these threats into three categories: cyber, physical, and climate change related. It's in our DNA to think about threats and to think about how we prevent the threats from occurring, but also then how do we recover should an issue occur? How do we make our system more resilient and more easily recoverable?

Cyber and physical attacks are really the main vectors into our systems. There was a cyber incident on the Colonial Pipeline several years ago, for instance. All the utilities are seeing cyber-attack threats from people trying to get into our systems.

But also from a physical standpoint, there were attacks recently on the substations in North Carolina, as well as a thwarted attempt where some folks wanted to attack the substations and cause outages in the Baltimore area. So again, it's all about doing everything we can to prevent the attack from being successful.

Because these are all ongoing threats, we have to work to be able to address each of them. Anything that could impact safety or reliability we treat very seriously. We do everything we can to put in place processes for each of those, whether it's climate, whether it's cyber-attacks, or whether it's physical attacks. They each require a different set of processes, procedures, and readiness, but those are all related to how you deter people, how you detect them, and how you delay their ability to attack. You assess the situation, you communicate, and you respond. That's the way we think about the problem.

Jay Owen: The grid is a prime target for sophisticated actors and we're seeing a variety of tactics to do so. They're targeting supply chains. They're compromising cloud accounts. They're using emerging technologies like AI to try to find a way in. That leads to all sorts of attacks which could result in downtime, or information technology (IT) hostage-taking for ransomware. The attackers are often criminal organizations but we've had to address dangerous state capabilities as well. Two years ago, we worked with the Cybersecurity and Infrastructure Security Agency (CISA) to issue an advisory for INCONTROLLER—a state sponsored cyberattack to get into industrial control systems.

These attacks are happening as digitization and automation in the grid are accelerating rapidly for both IT and operational technology, and that means the attack surface of the grid is expanding.

Another major area of concern is the security of the supply chains for energy infrastructure. The industry recognizes this concern, and we can talk about steps being taken to mitigate it. The U.S. government also recognizes this concern, and the Department of Defense actually has people assigned to look at that and put processes in place to mitigate it on their end.

How would you describe the nature of the cyberthreat to the grid, and what concerns you the most?

Rafael Sosa: First, let's take a step back for a moment. Not long ago, the utility controlled 100% of the assets. That's not the reality anymore and we've seen a transformation in the grid. Consumers, in some cases, have control over a number of these assets. And that creates a much broader and more complex threat landscape, with a whole new set of challenges.

For instance, my mother can control her home's power generation through an app on her phone. And those connections are not as strict or as vetted as what utilities are used to. In the cyber threat landscape, this is a much wider attack surface. Bad actors now have more opportunities to breach the electric system and cause disruption on a massive scale—activities that are outside the utility's visibility and control.

And then there's the 500lb gorilla in the room: the development of artificial technologies. AI is enabling much more sophisticated attacks on the grid, exploiting vulnerabilities. There is a need to recognize that the only way to really protect against these kinds of AI-driven threats is to incorporate AI into our defense strategy as well. There is no way that the traditional cybersecurity methods we've been used to will be effective enough to counter the ever-evolving AI threats that are surfacing.

So, when we talk about contingency planning and self-healing networks, everything is shifting closer to the customer to ensure reliability. The resilient grid of tomorrow isn't about stronger poles and wires; it's about smarter systems that can think, adapt, and heal on their own. To have a truly flexible, configurable distribution circuit, you need to respond within one or two cycles. You can't wait for a person to make a decision—it has to be automated. The only way to respond that quickly is by integrating AI into the entire decision-making process.

Ben Trowbridge: Cyberattacks on utilities have become faster, more automated, and highly targeted. The number of technical threats identified per hour is in the hundreds of thousands. The question, however, is which of these thousands of identified threats and vulnerabilities actually apply to you.

These cyber-threats are also complex and evolving, and several significant types of threats have emerged, including: nation-state attacks that can compromise the integrity of the Bulk Electric Grid; AI-powered malware in which adversaries use AI to rapidly identify vulnerabilities, automate cyber intrusions, and evade traditional security measures in real-time; cybercriminals providing Ransomware-as-a-Service (RaaS) allowing even low-skill attackers to launch highly disruptive attacks on utilities; and supply chain exploits, taking advantage of hidden vulnerabilities in third-party vendor software and hardware.

AI has added another level of complexity and speed to the cybersecurity environment. It's all about automating and speeding up individual techniques, both defensive and offensive, particularly by bad actors. This speed and automation are also making traditional defenses increasingly obsolete.

What steps are being taken by stakeholders across the energy grid to build resilience?

David Velazquez: Because the threats continue to evolve, our collaboration with government and industry partners is important for understanding the threat environment. We also have an emergency response organization that can be stood up and we conduct regular drills.

One important effort is the GridEx exercise, which is a national exercise involving utilities, our local partners, government partners, as well as national partners to simulate broad scale attacks on the grid and how we respond to them. And then we find the lessons learned and how we go forward to implement them.

Exelon has also invested more than a billion dollars in physical security measures over the past decade. We prioritize our facilities based on which are most critical to the grid, giving the highest level of protection to the most important ones, and then working down from there. These security measures include things like new fencing, advanced detection equipment, alarm points, access controls, video recording, and reactive lighting. We've also stood up a 24-hour security operations center, which monitors not only cyber threats but also physical security. Essentially, we've got "eyes on glass" around the clock to monitor for threats and respond appropriately.

Another thing we've been doing, and I think this applies across the industry, is increasing our level of spare equipment. God forbid any equipment gets damaged due to a physical attack, but we've made sure we're prepared to respond appropriately. For example, when you look at the attention on substation attacks, we have mobile transformers—large pieces of equipment that we can move to a location if needed. We have a number of those available and can deploy them quickly if something happens to a substation.

Looking ahead, we're also thinking about our ability to replace all the major transformers in a station if there's a catastrophic event that takes out the whole substation. This wasn't something we were thinking about 15 years ago, but it's definitely part of our planning now.

There are also two industry-wide programs that that we participate in. The Edison Electric Institute runs one called STEP, which is the Spare Transformer Equipment Program. And that is a coordinated approach to increase the inventory of transformers and streamline how we can transfer those transformers.

There's also the RESTORE program, which stands for Regional Equipment Sharing for Transmission Outage Restoration. It's a program among transmission owners where equipment can be shared to help with restoration efforts.

On top of that, when it comes to climate change, we're investing hundreds of millions of dollars to upgrade and harden the system against stronger weather impacts. We're raising the standards we use, not just in terms of how we design the system but also how we build it to withstand more extreme conditions. And it's not just about high wind. Since we serve areas next to streams, rivers, and coastal zones, we also have to consider flooding risks.

So, we're making sure that both new equipment and existing infrastructure are located in a way that minimizes flood risk, like avoiding 100-year or 500-year floodplains. There's a lot going on, with a huge amount of investment, all aimed at ensuring the grid stays resilient.

Jay Owen: There's a couple ways to look at it. One is: how do we prevent things from happening? The industry players are working together to make sure that we're doing things in a way that mitigates the risk as much as possible, and we take a risk-based approach. We use a cyber risk register and key internal controls to address those risks.

For cyber-defense in particular, we have the National Institute of Standards and Technology (NIST) framework that applies to any organization, as well as specific cyber security standards for operational technology and automation and control systems outlined in IEC 62443 from the International Electrotechnical Commission (IEC). And just a few months ago, myself, along with several of my industry peers, were at an event where we endorsed Department of Energy (DOE) and White House cybersecurity principles.

A key part of these efforts are "Secure by Design" principles, for which there are international standards and certifications. For instance, we're certified to the IEC 62443-4-1 standard. That includes security and penetration, and testing and then disclosure of those vulnerabilities. Those are some of the things that we're doing in terms of making the products themselves more hardened.

All of those efforts speak to trying to prevent bad things from happening. But you still need a backup plan in case they happen.

Within the U.S. government segment of my company, where my team and I participate, we frequently see the phrase "energy security is national security." Building resiliency into the grid is one thing, but building an additional layer of resiliency into the electrical infrastructure on a military base as a backup plan is another way to mitigate these kinds of concerns.

One of the ways of doing that is the deployment and coordination of distributed energy resources. If you go back to 2011, California experienced the biggest grid outage in its history. That led leaders at Marine Core Air Station Miramar to start to think about how they could put in renewable energy systems to offset—and make more green—energy consumption on the base. Working with other energy partners, we designed, installed, and commissioned a microgrid that can supply power to flight operations and up to 100 mission critical buildings in the absence of utility power.

Resiliency is also crucial when dealing with and mitigating the fallout from extreme weather events. To me, what was most unexpected about Hurricane Helene and Hurricane Milton last Fall was the unpredicted impact on North Carolina. You wouldn't think of the mountains of North Carolina as a place you have to harden against hurricanes, but we are working with a local partner called the Footprint Project to deploy solar-powered microgrids to help in those disaster recovery scenarios.

How would you rate the level of coordination and information sharing across public and private energy grid stakeholders in addressing threats to the grid? Is there anything that could improve?

David Velazquez: Over the last decade, I've seen a huge increase in information sharing—not just among utilities, but also in coordination with the federal government. And I'll give credit to the government, specifically NERC, for being proactive in ensuring that communication and coordination are in place.

The government has also started recognizing that the energy industry—both electric and gas utilities—is part of critical infrastructure. They've begun sharing tools and offering support, particularly on the cyber front, and that's been a huge help.

One of the major developments in recent years was the formation of the Electricity Information Sharing and Analysis Center (E-ISAC), which has been critical in helping the industry stay informed quickly about any emerging issues. There's also the Electricity Subsector Coordinating Council (ESCC), which acts as the primary liaison between the industry and the federal government. It coordinates efforts as we prepare for and respond to events. For example, during the hurricanes that hit the southern U.S. last Fall, the ESCC played a key role in coordinating response efforts and determining where resources were needed.

We're also members of the Edison Electric Institute, the American Gas Association, and maintain close coordination with local government agencies involved in cyber and physical security. This includes federal agencies, as well as urban areas we serve, like Philadelphia and the District of Columbia, where our ties are particularly strong.

There's also the important role of standards-setting bodies. We comply with standards from the North American Electric Reliability Corporation (NERC), which includes both cybersecurity and physical security requirements for our substations and equipment, and we've adopted the NIST Cybersecurity Framework to ensure our cybersecurity practices are comprehensive and thoughtfully implemented across the entire organization.

We're working diligently in each of these areas to provide the maximum protection and resiliency for our system, ensuring it's prepared for any eventuality. There's no mission more important than ensuring our grid's safety and reliability, and we are on it 24/7 every day.

Jay Owen: From what I've seen, I think it's pretty high as it pertains to the hardening of products. I mentioned the work we've done with CISA and working on specific threats, and we've seen our industry peers do that. I think there's a lot of coordination in terms of hardening the grid itself and things that we can do to make sure that the products aren't vulnerable.

I think there's a little less being done on how we use distributed energy resources to provide a backup plan and offset some of the energy usage from the grid itself. Energy demand is outpacing

the planned supply, and one of the best ways to deal with that is the appropriate use of distributed energy resources. DOE estimates that the adoption of distributed energy resources represents an investment of between $340 and $610 billion per year between 2025 and 2030.

There's a heck of a lot of investment going out into these distributed energy resources, so the question becomes, how do we make sure they're being coordinated and used correctly?

There needs to be more work done towards making sure distributed energy resources are actually coordinated well—essentially making them into a microgrid—so they can interoperate with the grid and are supported as a form of resilience rather than a form of competition.

Rafael Sosa: When we think about the fundamental pace of change, it's happening so much faster now. When you have these technologies that are so capable and so massive, the rate at which information can flow has to be taken into consideration, and I think we still have a lot of room to improve collaboration.

Going back to behind-the-meter, for example, there's a paradigm shift occurring. We're seeing a fundamental transformation where critical supply is increasingly reliant on non-utility assets. How we incorporate that information sharing—how we get visibility in that side of the operation—is something that still needs more coordination between the stakeholders. It's an area that hasn't been fully addressed yet. I call this a "security reliance paradox" because as individuals become more resilient through distributed energy resource, our collective grid security could actually become more vulnerable.

Take, for example, the current NERC Critical Infrastructure Protection (CIP) cybersecurity standards. They mainly focus on the bulk power system, which is a low-likelihood, high-impact risk, and operates under federal oversight. It's a mature framework. But the new vulnerabilities we're talking about can now be exploited through assets that are much closer to the customer. Those assets fall under state-level jurisdiction, and the frameworks for cybersecurity in that space aren't as mature. There's a big opportunity to standardize those state-level cybersecurity frameworks to address distributed energy resources, and to mature them in the same way that NERC CIP standards have matured for the federal system.

In the short term, there are important standards for cybersecurity that should be followed, for example the Institute of Electrical and Electronics Engineers (IEEE)1547.3 standard provides a solid model for mandatory encryption requirements. But when we think long term, we also need to look at quantum-resistant communication protocols and AI-enabled threat detection.

Ben Trowbridge: There is valuable intelligence being shared by mechanisms like the E-ISAC, along with dozens of private threat intelligence provides. The dilemma is that while information may be shared, there is a question of whether there's anyone who can take action—and if so, whether they can act fast enough for it to be relevant.

But the independent and decentralized nature of utility cybersecurity creates significant inefficiencies in responding to threats. Once threat information is shared, each utility is still responsible for: manually interpreting and prioritizing threat intelligence alerts, determining if the reported threat applies to their infrastructure, and reacting independently, based on their budget, personnel, and technical maturity.

This decentralized response approach leads to inconsistencies in response and response times based on the resources any given utility can devote to cybersecurity.

Smaller municipal utilities often lack dedicated security personnel or funding and may not be able to address threats in a timely manner, or able to address them at all.

This approach also requires each individual utility to set up their own security operations center which is not only difficult for smaller utilities to justify in terms of the resource allocation, it's also a highly fragmented approach that limits the nation's overall ability to respond to the threat.

Instead of each utility standing up its own security operations center, utilities could establish a network of regional or national security centers operated by cybersecurity firms certified for NERC CIP to provide real-time, 24/7 threat detection and response. Such an approach would be a more efficient use of cybersecurity resources as those resources would be pooled across multiple utilities to enhance grid-wide cyber-defense, while avoiding excessive duplication.

Even with such pooling, smaller utilities remain likely to struggle to devote sufficient resources to this growing challenge. The federal government should expand assistance to utilities so that they can modernize their cyber defense and adopt next-generation cybersecurity solutions.

How effective are current cybersecurity regulations for grid security?

Ben Trowbridge: The standards set by regulatory bodies like the NERC are incredibly effective from a compliance perspective. They are well-structured and thoughtfully designed, and utilities are on top of their compliance responsibilities.

NERC CIP standards provide a comprehensive baseline, and their value is undeniable. They establish a robust framework that addresses both physical and digital security, fostering significant accountability. You definitely don't want to fail a NERC CIP audit—it's a serious issue.

The challenge is that regulations have not evolved to keep up with today's cyber threats. NERC CIP regulations, for example, effectively prohibit cloud storage and external access to critical infrastructure data, making it impossible for utilities to adopt third-party, AI-driven and cloud-based cybersecurity solutions such as managed detection and response solutions that are standard in other sectors.

That means that the most valuable parts of the grid, the parts deemed "critical," can't take advantage of the most modern cyber security resources able to detect, analyze, and mitigate attacks in real time. This prohibition was originally intended to ensure only vetted persons could access critical systems.

However, that was before cyber-defense services moved to the cloud, became so complex and economically unfeasible for small and medium-sized utilities to individually defend against modern cyber threats.

We are long past due for regulatory modernization of critical infrastructure protection standards for the electric grid. The Federal Energy Regulatory Commission (FERC) has considered updating these standards for years.

However, even if approved today, compliance delays would still leave utilities years behind evolving threats. Immediate action is needed to avoid a scenario in which our utilities are unprepared and unable to defend against AI-driven cyber threats.

Once regulations are updated to reflect the modern threat, utilities will be able to adapt and evolve their cybersecurity defenses, engage qualified, vetted service providers, or build out a shared industry cybersecurity operations center with access to modern cloud services. The time for action and modernization is now.

Last Fall we saw Florida and the Southeast get hit with two back-to-back hurricanes that challenged response efforts and affected unexpected regions like western North Carolina. What are the lessons we need to learn to help build resilience against such events?

Rafael Sosa: That question really gets to the heart of the issue when it comes to responding and recovering. What we're seeing isn't just a series of isolated weather events. Take Puerto Rico, for example. When Hurricane Maria hit in 2017, it wasn't the first storm—they were hit by Irma just two weeks earlier. Irma brought in a lot of water and wind, which blasted an already ailing infrastructure. By the time Maria arrived, it just wiped everything out.

Now, look at the parallel with Florida in 2024. Just seven years later, we see Hurricane Helene, followed by Hurricane Milton hitting exactly two weeks apart. It's the same scenario. It's a striking and sobering parallel.

The painful reality is that our current regulatory and response framework was designed for a different era—back when such disasters were rare and not sequential. But today, we're facing crisis after crisis, and in my experience, there's a clear disconnect between utilities, state, and federal agencies. There's this maze of applications, reviews, and approvals that slows everything down. Meanwhile, communities continue to suffer.

I think the critical lesson here is that transparency and agility have to become the foundation of our disaster response framework. For instance, what if we incorporated blockchain to increase transparency in the process? We could track who submitted what, and where the delays are happening. Who's holding up the disaster relief from reaching the people who need it most? We need to see that kind of transparency to create accountability, and with that accountability, I believe we could have much more efficient responses.

AI-powered platforms could really help streamline application processes. When disaster strikes, paperwork should move faster than the storm clouds. But another thing we've seen is that people have lost trust in the utility, to some extent. When you look at Puerto Rico, there's a huge movement toward energy independence, where the customer has decided to install their own batteries and solar generation. It's a step toward greater resilience for the people there.

But ultimately, going back to my first point: the most important thing we need is agility in our regulatory processes. We need to have a faster, much more transparent response when it comes to disaster relief.

1030 15th St. NW · Suite 200 East
Washington, DC 20005
www.BENS.org | X: @BENS_org | 202.296.2125