IMEA
INDIANA MUNICIPAL ELECTRIC ASSOCIATION
SINCE 1941

eSource

Safety & Training Newsletter

January edition, 2023

Substation attacks may lead to new energy security rules in 2023, experts say

2022 ended with a series of physical substation attacks, but the cyber threat remains acute as well.

Robert Walton ***Senior Reporter*** ***Adeline Kon/Utility Dive***

Amid a growing cyber threat to the U.S. electric grid, 2022 ended with a spate of physical attacks that could portend new security rules for some energy infrastructure, say experts.

"The physical substation attacks toward the end of last year raised the alarm bell," Jason Christopher, director of cyber risk at Dragos, said in an email.

Multiple substations in Washington were damaged on Dec. 25, leading to more than 14,000 outages on the Tacoma Power and Puget Sound Energy systems. And a North Carolina firearms attack earlier in the month knocked power out to about 45,000 Duke Energy customers.

"Unfortunately, with 55,000 substations nationally, there are obvious risk-based limitations on addressing physical threats that need to be managed," Christopher said. "The industry should expect further regulatory inquiries and potential actions from the federal government in response."

The North American Electric Reliability Corp. oversees a set of critical infrastructure protection standards, known as CIP, governing rules for Bulk Electric System power equipment.

"I am hearing rumors that [the Federal Energy Regulatory Commission] may require NERC and the industry to revisit CIP-014, which is the physical standard for critical BES transmission substations," Kevin Perry, former director of infrastructure protection at Southwest Power Pool, said in an email.

FERC could consider stricter rules for more subs tations that operate between 200 kV and 499 kV, said Perry.

But he added, "I don't see FERC mandating costly physical security protections for those substations that engineering studies determine do not have a significant reliability impact if damaged or destroyed."

Cost is a major barrier to improving physical security, experts agreed, particularly because grid equipment is often in remote areas and the electric system is designed with redundancies in place. Loss of a single substation, for instance, should not cause an outage.

"What are you gonna do wrap everything in Kevlar? That would be a very poor use of regulation, in my opinion," said Thomas Pace, CEO and co-founder of NetRise.

While physical attacks may have grabbed headlines, the cyber threat is growing and hackers in Russia, China, Iran and North Korea all have sophisticated hacking abilities, say experts. And the rise of distributed energy resources creates a larger attack surface.

The Federal Energy Regulatory Commission is considering developing new cybersecurity rules for DERs on the bulk electric system, and the U.S. Department of Energy is funding "next-generation" cybersecurity research, development and demonstration projects.

Continued, Page2

(Continued)

Pace formerly worked with DOE, where he focused on industrial control systems security and said he expects more focus on software security in the coming year. That could include the potential for a software bill of materials, or SBOM, to be required for some vendors of some energy or grid-related services. The requirements would likely be "very prescriptive," he said.

Modern software is constructed of many components, making vulnerabilities difficult to track, say experts. The federal government and the electric power sector are collaborating on an initiative to more readily disclose what components go into grid software.

"I predict that the biggest cyber threat to the power industry in 2023 won't be direct hacks like those depicted in the movies, but supply chain attacks, especially those that come through software," said independent security consultant Tom Alrich. "These are currently the least understood of cyberattacks, and aren't directly covered by the NERC CIP standards."

Electric utilities "should be prepared for the increasing sophistication of supply chain compromise threats," Roya Gordon, a security expert at Nozomi Networks, said in an email.

NERC has scheduled a meeting in February and its Compliance Committee and Technology & Security Committee are both scheduled to make presentations. "They will likely be considering the role of technology and security in the ability for electric utilities to be compliant," Gordon said. "Let's be on the lookout for further NERC guidance after their February meetings."

"I suspect we will see some enhancements to NERC [requirements] in regards to supply chain cybersecurity, but mostly I think they will be clarifications vs. additions," said Ron Brash, vice president of technical research and integrations at aDolus Technology.

Brash also pointed to the importance of software security. "Asset management systems will begin to incorporate SBOMs to provide high-granularity visibility into the software and firmware running on assets," he said.

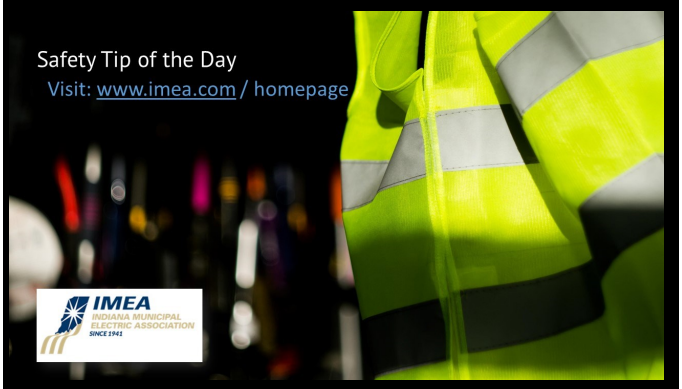
And there is a threat that supply chain constraints combine with grid attacks to exacerbate the impacts of any disruption, said Ron Fabela, chief technology officer of cybersecurity firm SynSaber.

"Supply chain globalization and just-in-time manufacturing [have] been an enduring challenge for the electric sector," Fabela said in an email. "An increase in physical attacks to grid components would exacerbate the issue, further amplified by any cyber disruption of suppliers through ransomware attacks."

Cyber risks that impact operations will continue to gain attention from utility leaders, especially if the Securities and Exchange Commission finalizes new rules on cybersecurity risk and incident disclosure that would impact investor-owned utilities, said Christopher.

"Those would force boards of directors to have specific expertise on cyber risk management, including understanding the impacts associated with cyber events," he said. "This could have a ripple effect across our industry and could shed additional light on the effectiveness of OT security programs and any potential resource constraints."

Visit the IMEA website for daily safety tips! Just go to: www.imea.com / IMEA Safety Tip of the Day and click on the topic link. This is a great opportunity to begin safety tailgate talks with your utility crew & staff at the beginning of each day and as always SAFETY IS A PRIORITY! #safetyfirst #safety



2023 IMEA CALENDAR

February		
15 - 16	*Supervisor Safety*	*Auburn*
March		
8 - 10	*Apprentice Top-Out Exam*	*Scottsburg*
13—17	*IMEA 613 Advanced Workshop*	*Scottsburg*
20—31	*IMEA 610 Wood Pole Climbing Workshop*	*Scottsburg*
April		
24 - 28	*IMEA 612 Intermediate Workshop*	*Scottsburg*
May		
8 – 12	*IMEA 611 Basic Workshop*	*Scottsburg*
24 – 25	*Line Clearance Arborist Certification*	*Frankfort*
June		
6 – 8	*Transformer Theory & Connections*	*Scottsburg*
28	*Distribution Devices Workshop*	*Lebanon*
16 – 21	*APPA National Conference*	
July		
6	*Excavation Competent Person Workshop*	*Auburn*
19 – 20	*Working it Hot Insolate & Isolate*	*Scottsburg*
August		
1 - 3	*Introduction to Supervision*	*Frankfort*
21 - 25	*611 Basic Workshop*	*Scottsburg*

Jobs in Public Power

Public power is more to communities than just an essential utility. It is a source of unique and fulfilling career opportunities in your local community. Employees make a difference by serving their own neighborhoods and families. Talented high school, college and technical college graduates—and even technology, environmental and public service professionals—will find that competitive salaries aren't the only thing attractive about careers in public power.

To post a classified ad to our jobs in Public Power page. Please email text to janel@imea.com.

Do you have important news or photos that you would like to share in our bi-weekly newsletters? Please email all news and photos to janel@imea.com

INDIANA MUNICIPAL ELECTRIC ASSOCIATION
176 W. LOGAN ST. #225
NOBLESVILLE, IN. 46060
765.366.5506 | imeainfo@imea.com