

Cybersecurity and Physical Security

Public power officials detail lessons learned from grid exercise

November 25, 2019

[Paul Ciampoli](#)

Officials from Salt River Project, CPS Energy and City Utilities of Springfield, Mo., on Nov. 19 detailed lessons their utilities learned from GridEx, a grid security exercise held this month that is designed for utilities to exercise their response and recovery to cyber and physical security threats in a simulated environment.

The officials made their comments at the American Public Power Association’s Cybersecurity Summit in Nashville, Tenn.

Participants on the panel, “GridEx V: What Did We Learn?,” were Warren Brooks, Supervisor-Substation Engineering, City Utilities of Springfield; Ken Lewis, Principal Planning Analyst, Business Continuity & Emergency Management, Arizona-based SRP; and Brandon Pixley, Director, Threat Intel & Security Awareness, Texas-based CPS Energy.

GridEx, which takes place every two years, allows utilities, government partners and other critical infrastructure participants to engage with local and regional first responders, exercise cross-sector impacts, improve unity of messages and communication, identify lessons learned and engage senior leadership.

The exercise began in 2011 and the North American Electric Reliability Corporation hosts the GridEx series. The 2019 GridEx marked the fifth such exercise.

There was a [big jump](#) in public power participation from GridEx IV to GridEx V, from 53 public power utilities in 2017 to 100 in 2019.

Officials detail lessons learned

At the cybersecurity summit, Brooks, Lewis and Pixley detailed how they and staff at their respective utilities approached GridEx V and the lessons learned from the exercise.

City Utilities of Springfield, Mo.

Brooks noted that one of the changes that City Utilities implemented from the last GridEx was to place utility staff participating in the exercise in one room.

In the room for the exercise were power generation, operations, and IT personnel, gas operations, communications personnel as well as planners.

“It was useful to have everyone in the room together and it also helped to avoid some distractions,” he said.

Brooks said that in terms of lessons learned, the key lesson is that the utility realized the benefit of having planners that were subject matter experts.

Another lesson that Brooks pointed to is the need to “customize this scenario. It really needs to be applicable to your utility,” he said.

In terms of the next GridEx, Brooks pointed out that while there are some benefits to having all exercise participants in one room, there are also some weaknesses.

“All of these folks that are actually going to respond are not going to all be in the same place together,” he said. “They’re going to be out in the field doing what they have to do with their resources and their personnel.”

Therefore, Brooks said that for the next GridEx, it is likely that City Utilities will have groups of exercise participants who will “team up in their respective areas and as long as we’ve tightened the communication up, that’ll get us a little bit closer to what we experience in a real scenario.”

SRP

SRP’s Lewis noted that the Arizona public power utility observed GridEx III, while for GridEx IV, there were 110 players.

For GridEx V, SRP had 185 players, with several new departments added to the exercise.

“We started planning back in April,” Lewis noted. “We basically got our planning team together, got our subject matter experts from all the different divisions and started to get together and say, what are we going to do this time that’s going to be different from what we did in 2017?”

He tells GridEx players “if you do everything right, we have designed the wrong exercise.”

Among the differences between the 2017 and 2019 SRP GridEx was the activation of the utility’s crisis management team. The crisis management team was simulated in the 2017 GridEx for SRP.

The crisis management team at SRP consists of senior leaders who staff and direct emergency response for corporate level events. It is an all-hazards team that can address a wide range of events including an active shooter, rotating outages, a cyber hack or a pandemic.

During the 2019 exercise, Lewis said that the players were “very, very engaged,” with a high level of activity in terms of phone call and email traffic.

Lewis also detailed where SRP excelled. He said that the technology worked, including email, the SimulationDeck provided for the exercise and the Electricity Information Sharing and Analysis Center mirrored system.

Moreover, the injects for the exercise were well thought out. “We actually did engineering studies. We looked at November thirteenth and fourteenth in our history, found out what the load was” in order to determine “what kind of mayhem are we going to have to cause to get to the point that we would be forced into rotating outages,” Lewis said.

Positive exercise feedback from players included:

- Great content;
- Highly interactive scenarios;
- Strong replication of real-time scenarios with inter-departmental interaction;
- Subject matter experts involved had the knowledge and skills to work through scenarios;

- Tools provided through GridEx were valuable including the SimulationDeck and videos; and
- Hugely beneficial to train for situations that truly could occur

CPS Energy

CPS Energy's Pixley said that with respect to GridEx V objectives, the utility wanted to, among other things, expand its local and regional response capabilities.

CPS Energy wanted to practice response management in a multi-agency response environment. "That means, how are we going to work with San Antonio Fire Department and how are we going to work with San Antonio Police Department?" Pixley noted. "Are we able to work together with the various agencies while handling multiple incidents? And, then also, how will the FBI play a role?" Once there are multiple groups "all working together it gets difficult to manage and so we were trying to test that."

In addition, the utility was focused on evaluating the readiness of response resources. "That simply means, is everyone actually able to do what we say they are going to do."

In addition, CPS Energy wanted to practice live media and a public affairs response in GridEx V.

"What we did this time is we actually set up cameras" and placed relevant exercise participants "in front of a camera and we mocked up some news reporters and then people were asking questions and then we broadcasted that live," Pixley said.

He said that this was extremely useful for the utility to do. Some people had limited time in front of a camera with people asking them questions.

Pixley said that in terms of GridEx V lessons learned from a strength perspective, there was a team emphasis on safety.

Also, the crisis management plan matured. The original procedure "grew into a much bigger crisis management plan – that was very impactful, so I can't stress it enough. If you guys don't have a crisis management plan you need to think about it. There's plenty of information out there on how to develop one."

Another lesson learned from a strength perspective was prioritizing customer engagement. "We practiced things going out" on social media to let CPS Energy customers know what was actually happening, the CPS Energy official said.

As for areas for improvement, Pixley noted that rapid injects during the exercise resulted in "analysis paralysis." He said that "the teams were overanalyzing everything that was going on, trying to solve it all, trying to figure out what's happening." Ultimately, the teams missed the correlation of the events or the bigger picture.

Pixley said he would also like to have bigger response teams during GridEx.

"If I only have two incident responders but in reality I'll have eight, how is that fair to those incident responders? They're not going to know how to actually handle the incident because all their team members aren't there. So if you're going to do this and you're going to put in a lot of injects, make sure that you have everyone available at your disposal for your teams because they're actually going to be able to test how they normally would act."

Association's Rozenberg emphasizes that GridEx is scalable event

Sam Rozenberg, Engineering Services Security Director, said that it is important to note that GridEx is a scalable exercise.

“I just want to emphasize that GridEx and other exercises are not just for the big players, are not just for large organizations, they're for every organization – you just have to work on customizing it.”

Rozenberg also asked audience members to think about whether there is anything more the Association can do to help public power distribution utilities that are small participate in a GridEx-like exercise.

“We'll probably be reaching out for some input on that,” he said.