Duke has 'very detailed' cyber security plan

BY GREG OLIVER
THE JOURNAL

SENECA — Nuclear power plants have long been designed to protect against incidents — including radiological accidents and the use of weapons or explosive devices — that could pose a threat to public safety.

While the 9/11 attacks contained no cyber component, the nuclear industry took the initiative from the tragedy to implement a cyber security program. Officials said the program is designed to maintain nuclear safety and continuity of electric power.

In 2002, the Nuclear Energy Institute formed a task force to develop cyber security guidelines for the industry — reviewing cyber security measures at four nuclear power plants and testing potential vulnerabilities. The Nuclear Regulatory Commission endorsed the industry guidelines in 2005 and, by May 2008, all 104 operating plants had implemented them voluntarily.

Sandra Magee, spokesperson for Duke Energy, said the company has "a very detailed" cyber security plan for all of its facilities.

"We update, plan and implement new standards and controls as needed," Magee said.

Magee added that information technology officials monitor the system 24/7 to ensure safety and security of its massive data.

"There is a multi-layered defense approach that helps protect our business and our information technology assets, such as our network system, computer system and everything involving information and data," she said. "We also partner with cyber security vendors and providers that provide a lot of guidance and beneficial information.

"But we don't just depend on that, because we have our own cyber security professionals. These individuals are very highly skilled and this is their sole devotion to their work."



PHOTO COURTESY OF DUKE ENERGY

Experts say nuclear power plants, such as Duke Energy, are better equipped to defend against potentially devastating cyber attacks than most other utilities.

Potential threats from cyber attacks range from computer viruses and worms to unauthorized access to protected data and systems. These and other cyber-related threats have the potential to damage or shut down systems, destroy valuable information or compromise privacy and security — including radiological sabotage.

Cyber security plans must include measures to ensure the capability for timely detection and response to cyber attacks, to mitigate the consequences of such attacks, correct exploited vulnerabilities and restore the affected systems, networks and equipment.

Magee said nuclear power plants have additional layers of protection against cyber attacks compared to most businesses.

"Whereas a lot of businesses, such as banking, require two-way data flow, that is something we don't require since it (data) is being generated by our operating plant," she said.

In addition, Magee said the safety and control system at Duke is not connected to the Internet and there are no problems regarding identity theft.

"The need for data information and security is very important in our business, and we invest in the newest in technologies to ensure we have that," she said.

greg@dailyjm.com | (864) 973-6687