



Don Horne

CYBER SECURITY AS IMPORTANT AS A GOOD CHAIN LINK FENCE

Cyber security. Protecting substations, transmission and distribution corridors and other utility assets now goes beyond chain link fence, security cameras and locked doors.

Now potential threats are coming literally in the ether – the Ethernet.

Verano's recent rebranding announcement (they are now Industrial Defender) underlines the shift in priorities for many utilities, as they begin devoting larger portions of their operating budgets to installing or upgrading their cyber security systems.

Industrial Defender marks the commitment of what was once Verano to the identification, mitigation and prevention of cyber-threats to power, water, energy, transportation and chemical industries. Critical infrastructure cyber security is becoming as important as maintaining transmission cable integrity to ensure a fully functioning network.

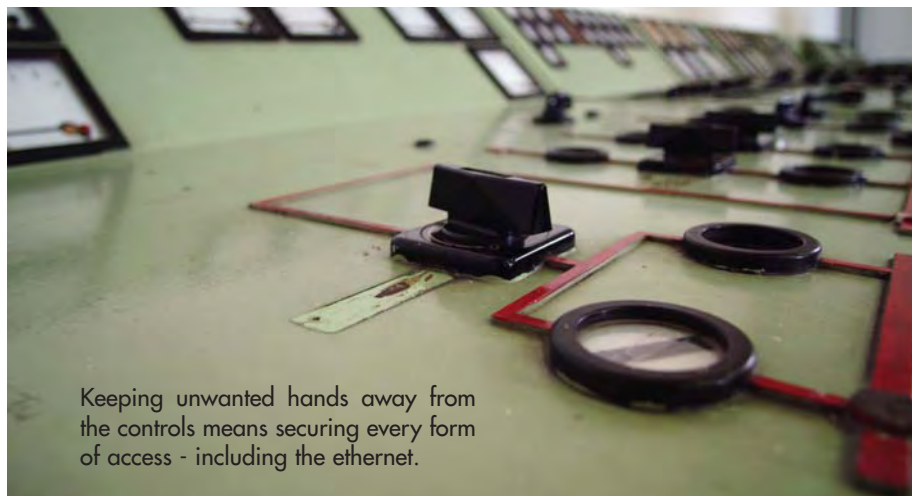
An August 2006 shutdown at the Browns Ferry Unit 3 nuclear facility in northern Alabama came under closer scrutiny from two leading Democratic Congressmen, who sent a letter to the chairman of the U.S. Nuclear Regulatory Commission (NRC) calling for an investigation into the nation's nuclear cyber-security.

The letter, sent in mid-May, described the 2006 shutdown as a cyber security incident.

The northern Alabama Unit 3 facility was manually shut down following the loss of both of the recirculation pumps (two nuclear generating units are located at Browns Ferry).

According to the letter, the plant personnel determined that the cause of the failure was due to "excessive traffic" on the computer network. As a corrective measure, a firewall was placed on the plant's integrated computer system network.

The NRC followed regulations and decided not to investigate the failure as a cybersecurity incident because the failing system was a "non-safety" system and



Keeping unwanted hands away from the controls means securing every form of access - including the ethernet.

the licensee (the nuclear plant in question) had determined that the incident did not involve an external cyber attack on the system.

But the two Democrats, Committee on Homeland Security chairman Bennie G. Thompson, D-Miss., and Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology chairman James R. Langevin D-R.I. had "deep reservations" about the decision not to investigate the incident, adding that the Browns Ferry shutdown revealed that non-safety system can affect plant safety.

And there remains doubts as to whether there was any hacking of the system.

"Conversations between the Homeland Security Committee staff and NRC representatives suggest that it is possible that this incident could have come from outside the plant," reads the letter. "Unless and until the cause of the excessive network load can be explained, there is no way for either the licensee or the NRC to know that this was not an external distributed denial-of-service attack. Without a thorough, independent review of the logs and associated data, the assumption that this incident is not an outside attack is unjustifiable."

The congressmen have requested a further investigation of the source of the

"data storm" by the NRC.

As detailed in the Industrial Defender story in this issue, there is an excellent example of the California man now facing charges of sabotage when he attempted to access the Cal-ISO computer network (after being denied access, he instead pushed an emergency shut-off that created a small blackout and crashed computers used to communicate with the power market).

Viewed as an unsuccessful attempt to sabotage the system, it nonetheless required 20 computer technicians working seven hours to restore the systems.

Utilities are faced with the mammoth task of updating and upgrading a massive infrastructure consisting of lines, towers and equipment that, in some cases, is more than twice the age of the young men and women working on them. New SCADA and computer communication networks also carry hefty pricetags, so paying that much more to ensure their safety and security can be viewed as a luxury.

But as we've seen with frightening regularity each and every night on the news, there are those people out there who are ready, willing and able to spread terror and chaos – and where better than through the very system that keeps the wheels of commerce turning?

don@electricityforum.com