Emergency Security

SANS SCADA Summit
Orlando, FL
February 2-3, 2009

Thomas R. Flowers, P.E.
President
Control Center Solutions, LLC
(Sponsored by DOE)

Emergency Preparation in the Critical Sectors

Most Critical Sectors:

- Must prepare for and respond to emergencies
- Have an Emergency Operations Plan or equivalent
- Have a chapter in their EOP covering shut down and evacuation

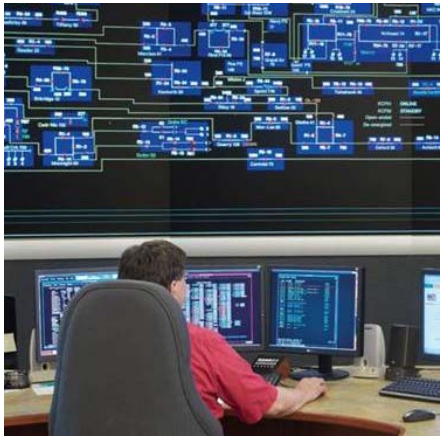
… except one

The Electric Sector

"If a segment of the Electric Sector shuts down, that's an emergency. If a segment of the Electric Sector shuts down during an emergency, that's a disaster."

T.R. Flowers, P.E.

The Platform



The Control Center is similar to an aircraft carrier. Both must:

- Have the stand-alone capacity to perform mission critical operations in the worst of conditions
- Provide a secure and resilient environment for its operating personnel and infrastructure
- Be capable of sustaining operations indefinitely using the latest technologies

The Platform

Imagine if just prior to “Top Gun” type operations on a carrier, that a ship full of Generals, Admirals, Congressmen, and all their staff came aboard to help.

The Problem

Prior to an emergency like Rita or Ike, a small army of engineers, managers, and executives will show up at your Control Center with a roll of substation schematics under one arm and a dirty laptop under the other.

The Solution

- Get a notice out to all expected “Guests” with instructions on how to “clean” their laptops prior to the annual EOP Drill
- Inform all potential Guests of the physical and cyber security procedures they can expect when they arrive at the Control Center for EOP duty
- Implement a process that insures every Guest laptop undergoes a standardized security audit and is returned to the Guest afterward with a conspicuous audit sticker affixed
- Establish Guest zones similar to small DMZs using firewalls, VPNs, and smart switches

The Solution

- Implement IDS/IPS and other monitoring and control technologies on these Guest zones independent from the ESP monitoring and control technologies in place for your critical networks
- Establish Port Security on all communication network ports across the entire ESP leaving only the Guest zones unrestricted
- Monitor all wireless use within the ESP where possible given the limited technology to do so

The Solution

- Provide all peripheral devices needed by the Guests within the Guest zones
- Train all Control Center personnel to “greet” all Guests if they are not prominently displaying approved ID
- Leave Contact, Trouble, FAQ, and EOP process material in the Guest zones for reference
- Incorporate all of the above into the annual EOP Drill

The Tricks

Don’t reduce or adjust any aspect of your physical or cyber security processes or policies for the duration of the EOP event

- Use legacy equipment and reconfigure it for Guest zone use where possible
- Pre-stage materials, pre-configure offices/conference rooms to be used for Guest zones, and have your support staff make regular fly-bys to all zones to provide Guest service particularly in the first 36 hours
- Expect some level of contamination, at some point, in one or more of your Guest zones and incorporate the response to this in your annual EOP Drill
- More compartmentalization between Guest zones is better than less for containment and incident response purposes

Contact Information

Thomas R. Flowers, P.E.
President
Flowers Control Center Solutions, LLC
936-894-3649 office
281-900-9041 mobile
flowersccs@att.net

Questions?