



Illena Armstrong

Start spending today to avoid chaos tomorrow

Now that the lights are back on in much of the Northeast and Canada, a spotlight is being cast on a game of finger-pointing.

As of press time, most officials are reportedly focusing on an Ohio utility company, FirstEnergy Corp., saying failures in its high-voltage lines triggered the biggest blackout in U.S. history. However, officials there are reportedly claiming that they witnessed unusual spikes and lows in voltage throughout the Midwest grid several hours before the power outage hit its peak at 4:11 PM EDT time on August 14.

For now, most utilities officials, including those with the North American Electric Reliability Council (NERC), whose president Michehl Gent voiced embarrassment at the outage, are all saying its too soon to say for certain what the main cause of the outage was. It'll likely be some time before we know exactly what went down.

Initial reports stated that the Blaster worm was responsible for taking out the networks supporting the grid, but NERC's Gent quickly dispelled that postulation. However, some reports imply that perhaps government officials were premature in suggesting that a computer worm was not to blame for the wide disruption, since various failures were shown to occur at multiple locations and times throughout the grid - happenings that could support a worm making its way across the interconnected systems.

Whatever the trigger turns out to be, there is no doubting the impact a worm could do - let's not even talk about a hacking incident combined with a terrorist attack. Indeed, this outage, which covered a region across some eight states, shows just how reliant we are on power and how vulnerable we are to its loss.

So, what should utility companies, other critical infrastructure enterprises and the government be doing? Adam Lipson, with Network & Security Technologies in New York, says that the nation's electric power industry is supporting standards development. "Just this week NERC ratified its Cyber Security Standard that covers all entities associated with the power grid. In fact, however, many of them have a long road ahead to achieve compliance," he says.

Although the standards are not difficult to implement, adds Lipson, few companies have actually adopted them. Because of this, "considerable money, resources and time will be required to improve cybersecurity. Executive support is essential to accelerating these efforts."

If that's what it will take, then critical infrastructure companies, as well as associated government entities, better get jumping - no matter the initial capital outlay. Most reports show losses in the millions for employers in the various states affected by this event alone. And, we've already witnessed the devastating effects of 9/11. We're seeing what today can bring. Tomorrow could be much worse.

Perhaps officials were premature in saying that a computer worm was not to blame for the wide disruption.

Illena Armstrong is US and Features Editor