YET ANOTHER EDITION OF “YOU WERE WARNED”

Dear unnamed power company/ies: Thank you for providing me an opportunity to post one of my favorite videos.

AGAIN.

You were warned about the possibility of security threats to your systems. Repeatedly—the video above is just one such warning. What’s it take to get through to you—a clue-by-four alongside the head? A massive, lengthy power outage you can’t resolve for days or weeks, with consumers calling for managements’ heads on pikes? A complete tank of your company’s stock value? The Department of Energy on your doorstep, taking possession of your site as it investigates you?

I love this part at 32:28 into the video where Ralf Langer says,

> “…many things we thought about cyberwarfare earlier just were proven wrong. …”

Everything you thought you knew about infosec/cybersecurity needs to be revisited. The assumptions you’ve been using are clearly wrong.

Now get a frigging clue and revisit your security policies. STAT. You can start with checking these:

— No USB or other external media which have not been deeply screened for infection.

— External network connections to production equipment are to be avoided at all costs. Connections between corporate business and the power grid should be closed, dedicated network. Revisiting appropriateness of traditional isolation of production networks might be worthwhile.

– No third-party contractors permitted on site that do not comply completely with power company security policies, including spot inspections. (You do spot inspections, right? Contractors are screened coming in and out of facilities, right?)

What are you doing here, reading this? Get to work. RUN.

Dear U.S. Department of Energy: Um, hello? Did your brains' functions suffer irreparable damage from exposure to BP's dispersants?

It's the only excuse I can think of as to why security measures and subsequent audits of the nation's power grid for infections and intrusions from network and external devices haven't removed these threats.

By the way, this 2009 document making suggestions to power companies about security measures is now out of date and needs to be revisited, in light of the Senate Intelligence Committee's authorization of cyber weapon deployment and subsequent blowback risk, let alone the case of USB devices laden with crimeware.

Dear Fellow Americans: I really hate feeling like Cassandra. I'd love to see the power industry and our government prove me wrong by preventing outages related to security breaches about which they've been warned. At the rate they're going, you're going to end up on the short end of the stick, without electricity to read my anticipated future post which I expect to entitle, "I told you so."

You might want to contact your government representatives and ask them what they know about power grid security and if they've actually done anything to investigate the safety of power in their district. If their understanding is shaped by the Department of Energy's latency, they need to be brought up to speed and pronto. Don't wait until you don't have the juice to read my next post on this topic.