Aleta Technologies, Inc.

Cybersecurity for the Power Grid
Alabama Power Grid Defense Conference

20 September 2016

Presented by:

Jay Kurowsky, President & CEO

256-895-8870

jay.kurowsky@aletatechnologies.com

Aleta Technologies, Inc.

Who am I?

(i.e. why am I at least semi-credible?)

- 20 years' experience in cybersecurity/information security and related fields, including support to Information Warfare
- 19 year's experience writing DoD Information Security/ cybersecurity regulations
- Served on behalf of the Pentagon determining what systems were and were not sufficiently secure to connect to the Army's tactical communications network
- **Managed vulnerability assessment support to over 1,000 systems**
- Served as Army representative for Software Protection/Anti-tamper
- Helped pioneer Software Assurance for the Department of Defense, including determining policy and evaluating some of the Army's most sensitive software
- Recently served as the alternate Army representative for Risk Management Framework for RDT&E systems
- Currently helping global manufacturers secure their energy and industrial control systems

Aleta Technologies, Inc.

DISCLAIMER: **My company profits from cybersecurity.**

But hopefully you will listen to my briefing closely enough to decide for yourself if there is a problem with the state of cybersecurity of the U.S. power grid that is big enough for your attention, and hopefully you will decide to help.

Though I'm speaking on the bulk electric system, my experience is more geared to individual energy systems (plus some of the largest IT systems on the planet).

The State of Affairs: A Bad Fashion Trend

Overall, the U.S. bulk electric system, AKA the power grid, is in the same terrible cybersecurity state as the tactical battlefield was in the 1990s.

Don't believe it? Neither did the Pentagon in the 1990s, but they have since made MAJOR changes, and have named cyber as the fifth warfighting domain.

It's a good thing we've been at "peace" with peer adversaries.

Hopefully bell bottoms are on their way out again, too.

Aleta Technologies, Inc.

A Good Start….

- **The current standard for energy-related systems is compliance:**
  - **Risk Management Framework for DoD Information Technology (“the RMF”)**
  - **North American Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards**
- **The problem is, though much better than nothing, regulations take years to develop and encourage minimal compliance**

Aleta Technologies, Inc.

…but More is Needed

- **Despite efforts to the contrary, regulatory compliance frequently also encourages security measures to be "bolted on" at the end rather than "baked in" early in component and system development**

- **When security measures are bolted on, they are not only more expensive, but they also frequently shift burden from hardware and software to "wetware", which is far riskier**

Aleta Technologies, Inc.

Proof of Vulnerabilities

- **Numerous vulnerabilities to power grid products are reported each year, with the Department of Homeland Security Industrial Control System Cyber Emergency Response Team maintaining an extensive list at https://ics-cert.us-cert.gov/alerts**

- **The vulnerabilities worth losing sleep over are the ones that are not reported—the ones that Russia, North Korea, China, and others are secretly storing for a time they want to use them on our grid**

So you say Susceptibilities and Not Vulnerabilities?

- **Considering that a lengthy wide-scale outage of the power grid would cause massive loss of life, to say there is no documented threat seems like a very bad bet to me**

- **Beginning on 23 December 2015, Ukraine lost power to 225,000 people, and the U.S. Department of Energy, FBI, and others concluded that the outage was caused by remote cyber attackers**

Aleta Technologies, Inc.

Ukrainian Power Grid Attack

- **The attack included remote intrusions to ~3 regional electric power distribution companies that Ukrainian officials reported* as synchronized and coordinated, involving:**
  - **Malicious remote operation of breakers by external humans using either remote administration tools at the operating system level or remote industrial control system client software**
  - **Damaging human-machine interface and other systems with malware, rendering them inoperable**
  - **Rendering serial-to-Ethernet devices at substations inoperable by corrupting their firmware**
  - **Disconnecting server Uninterruptable Power Supplies via their remote management interface**

* https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

Ukrainian Power Grid Attack, Cont'd

- **Power was restored, mostly manually, though the systems reportedly ran under constrained operations for months**

- **Though this event did not cause large-scale loss of life, the results may have been worse in the U.S., and this event is just the start….**

Aleta Technologies, Inc.

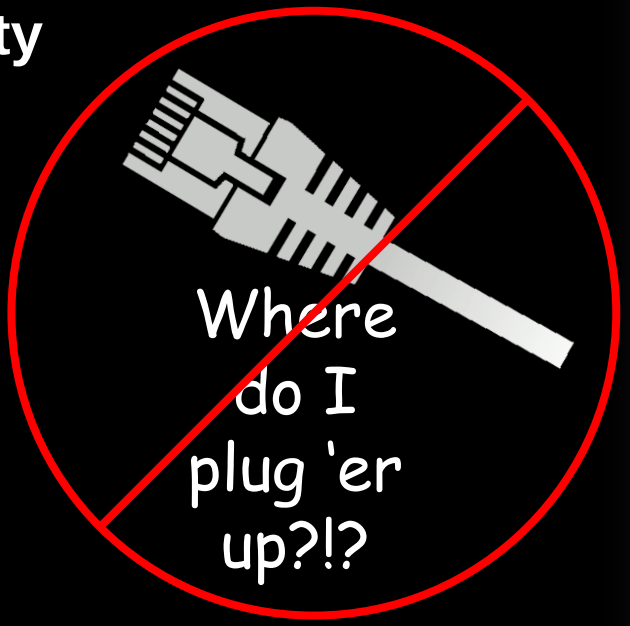
How Bad Could it Be?

One thing to keep in mind about cyber attacks is that nearly anything that can be imagined can be executed

So What Do We Do About It?

- **Manufacturers and system integrators are not going to achieve a suitable level of security "just because", especially when their competitors are not incurring those costs, and consumers are not demanding increased security**

- **Even just the current level of cybersecurity compliance exists because regulators have imposed it, customers have demanded it, and system acquirers have required it via contractual verbiage**



Demand More

- **We must demand more than just basic compliance—we must demand things like:**
  - **Robust and periodic penetration testing**
  - **Heavy-duty supply chain risk management**
  - **Secure software coding practice and malicious code assessment**
- **Product and system acquirers: If you are not a veteran cyber expert, you can't get the job done without a seasoned and well-rounded expert helping you from solicitation to installation and maintenance**

Get involved!

Or Else....

NO

VOLTAGE

Questions?