CYBER SECURITY

May 6, 2013

Cyber Headlines: dramatic and numerous

Burning up a generator on demand
Staged cyber attack reveals vulnerability in power grid, *CNN* 09/26/2007

Georgia Takes a Beating in the Cyberwar With Russia
New York Times 08/11/2008

Pro-Wikileaks Hackers Take Down MasterCard, Visa
(widely reported) Dec. 8, 2010

Stuxnet
New spy rootkit targets industrial secrets (Stuxnet) *Tech World,* 07/19/2010

Stuxnet virus targets and spread revealed *BBC News,* 02/15/2011

The Pandora's Box of Stuxnet, Duqu, and Flame *PC World* 06/01/2012

Cyber-attack claims at US water facility
The Guardian 11/20/2011

America's Failing Grade on Cyber Attack Readiness *ABC News* 07/27/2011

Hackers in China Attacked The Times for Last 4 Months, *New York Times* 01/30/2013

Will the next 9/11 be digital?
Digital Trends, 04/01/2013

South Korea Hit Hard by Massive Cyber Attack *PBS NewsHour* 04/01/2013 (on attacks from 03/20/2012

All those headlines => Government Response?

- Canada's response
  - Cybersecurity policy announced in 2001
  - Canada's auditor general reports little progress
  - In 2010 the federal government puts in place *Cyber Security Strategy and the National strategy and action plan for critical infrastructure*
  - Auditor general reports progress on relationship building but little definitive improvement 24/7 awareness and other key action items

But so far, no made-in-Canada stuxnet – or is Canada's stuxnet still a secret?

Why are we so cyber-vulnerable?

- Cyber-systems allow efficient control of complex systems
  - The more efficient and powerful these systems become, the more impact they can have when they are compromised.

Cyber-vulnerability

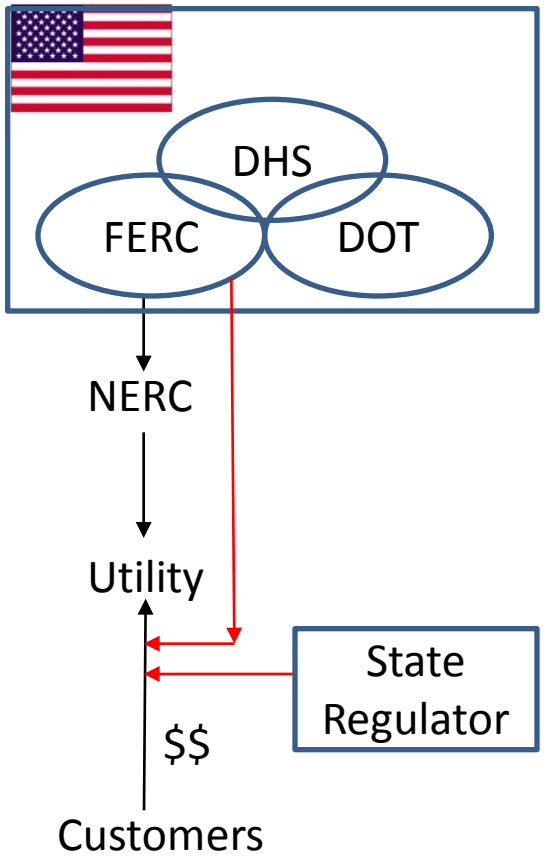
A cyber-vulnerability can

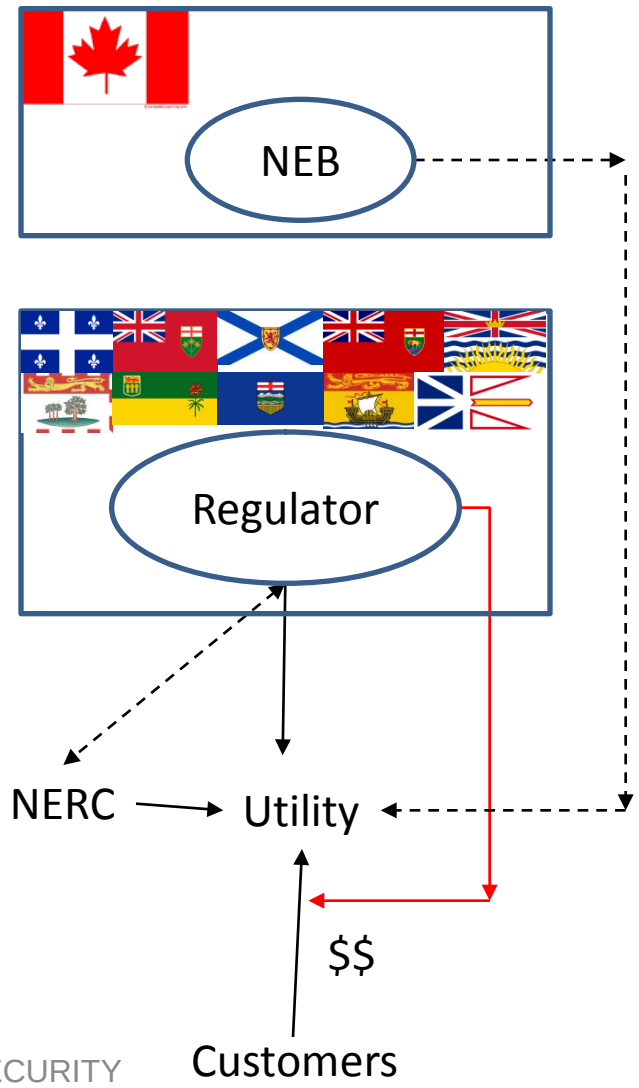
- be deliberately exploited to gain
  - Power (political/military)
  - Knowledge (espionage)
  - Money
  - Glory
  - Revenge (e.g. sabotage)
- break
  - Accidents, human error

Infrastructure security – Federal

- Headed by Public Safety Canada (Critical Infrastructure) and the RCMP
- Develop working relationships and find ways to share information within and between sectors
- 10 industrial sectors in Canada (18 in US)
  - Energy and Utilities sector is the most advanced.
- Structurally and in general orientation, US and Canada are deliberately similar and align with one another

Cyber Regulation of Electricity



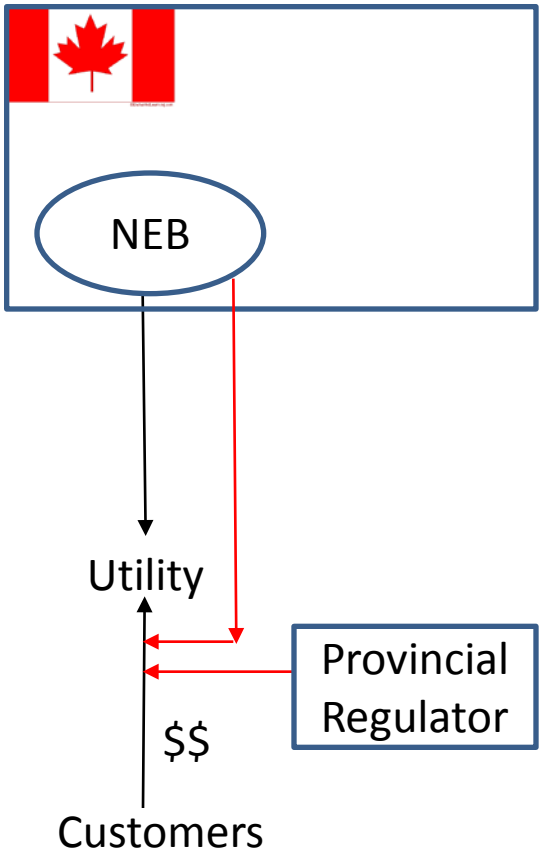


Electricity Cyber Regulation in Canada

- Generally following NERC Critical Infrastructure Protection standards
- Nationwide, different provinces are at different stages of NERC standards adoption
- Ontario has CIP version 3 in force, whereas in Québec, we have adopted CIP version 1 and are still developing the enforcement framework. Meanwhile, Hydro-Québec, Québec's principal utility, complies with CIP version 3 (and CIP version 1) on a voluntary basis until Québec's regulatory regime catches up.

Cyber Regulation of Natural Gas

International and interprovincial



Evolving dynamics

- In general, the power dynamic between FERC and an American utility is not the same as between a provincial regulator and a provincial utility.
- Generalizing substantially, Canadian regulation tends towards collaboration and meeting objectives. (e.g. "Tell us how you protect your cyber-infrastructure against significant risks?")
- However, Canadian regulation is trending towards more definition.
  - Electric industry alignment with a mandatory regime with fines
  - NEB's upcoming authority to levy fines for natural gas issues
- Meanwhile, American regulation is perhaps moving towards objective based (CIP5, NERC RAI)
- Perhaps Canadian regulation and American regulation will meet in some happy middle – that would be a very Canadian compromise!

- MERCI!
- THANK YOU!