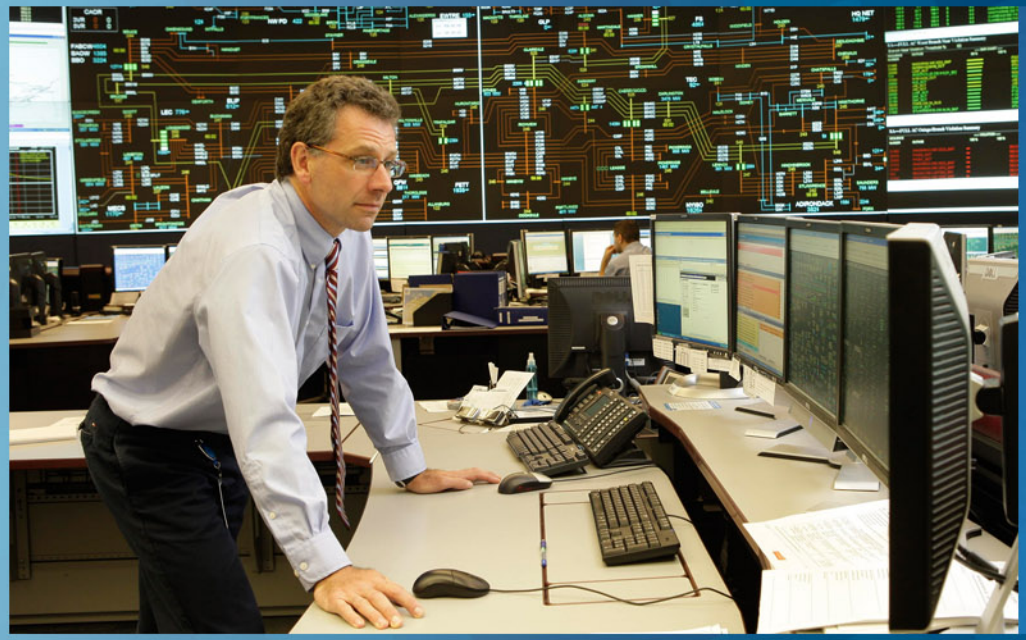
ieso
Power to Ontario.
On Demand.

Cybersecurity in Canada's electricity industry

Ben Blakely - Team Lead, Security & Enterprise Security Architect

October 22nd, 2013



Agenda

- Background
- Current Approach
- Future Positioning

Background

- What is cybersecurity in Canada?
  - Canadian legal jurisdiction of cybersecurity
  - Canada's Cybersecurity Strategy
    - Built on 3 pillars
  - Action Plan 2010-2015 for Canada's Cybersecurity Strategy

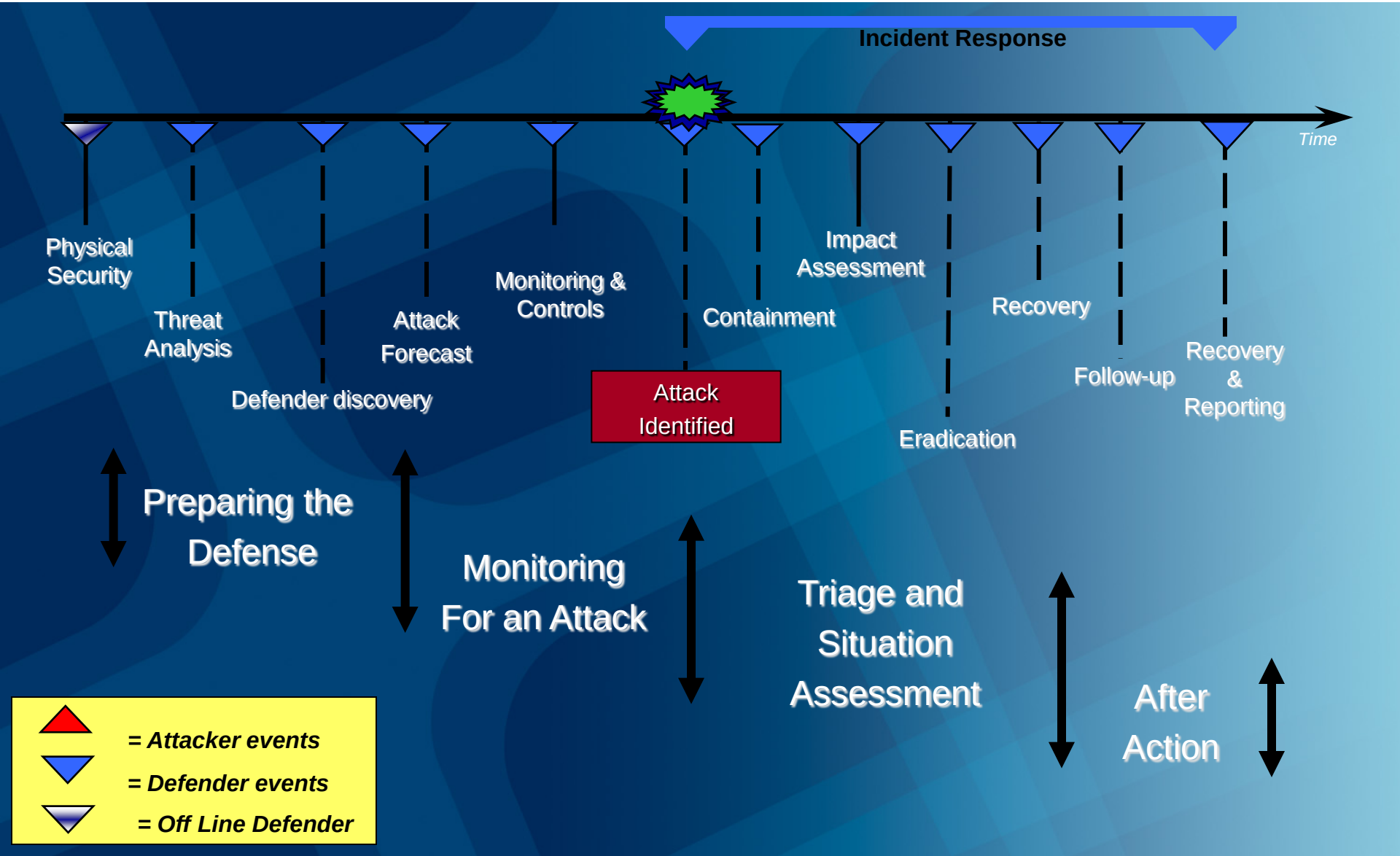
Canada's Cyber Action Plan- Progress in the electricity industry

- Pillar #2

  - Canada's Cyber Incident Management Framework
  - Cybersecurity briefings
  - CEO engagement
  - Security clearances
  - Information sharing arrangements and protocols
  - Workshops to improve awareness
  - Establish National Energy Infrastructure Test Center
  - Operate a ICS laboratory program and testing environment

  - Improve CCIRC ability to support non-federal government agencies*

A timeline of a cyber attack



Current Approach Dashboard

Framework for managing security issues: Green

	Status	Trend	Status
Preparation	G	↑	• Increase in industry security exercises
Identification	Y	↑	• Difficult to address crosscutting threats
Containment	G	▬	• No concerns at this time
Eradication	G	▬	• No concerns at this time
Recovery	Y	▬	• Difficult for organizations to be resilient against threat actors with resources (ex: Saudi Aramco, Rasgas (LNG producer in Qatar) scale attacks)
Follow-up	G	▬	• No concerns at this time
Reporting	Y	↑	• Increase Information Sharing to support rapid identification of threats

Future Position - Preparation

- IESO-led robust inter-sector security exercises
  - Exercise critical infrastructure information sharing protocols/procedures and participant response to Bulk Electric System cyber and physical security threats between the following sectors:
    - Government Entities
    - Electrical Grid Operations
    - Gas Industry
    - Telecommunications
  - Implement and communicate existing coordinated response reports to industry and government (Canadian Cyber Incident Response Centre (CCIRC), North-American Electric Reliability Corporation (NERC) and the Electricity Sector Information Sharing and Analysis Center (ES-ISAC).
  - Explore senior leadership policy decisions and triggers in response to major grid reliability issues and large scale security incidents through activation of the IESO Crisis Management Support Team (CMST) and Emergency Response Team (ERT).
  - Identify potential improvements in physical and cyber-security plans, programs, and responder skills.

Future Position - Preparation

- Ontario Market Participants
  - IESO
  - Hydro One
  - Ontario Power Generation
  - Bruce Power
  - Toronto Hydro
  - Hydro Ottawa
  - Brookfield
  - Great Lakes Power

- Ontario Supporting Agencies
  - Canadian Cyber Incident Response Center (CCIRC)
  - Royal Canadian Mounted Police, OINSET
  - CSIS
  - OPP, Critical Incident Command
  - Canadian Electricity Association
  - Ottawa Police Service
  - Durham Police Service
  - AllStream/Bell Canada
  - Union Gas/Enbridge

Future Positioning – Identification & Reporting

- Canadian Electricity Association (CEA), Security Incident Communications Plan
  - A process for collaborative incident response within Canada's electricity industry,
  - Identification of individuals in key security roles across the country that will notify others of incidents of low, medium and high severity through different means,
  - Align and fuse resources from industry & security/intelligence agencies to be the most effective in cybersecurity risk management.

Future Position - Identification

- Ontario Electricity Cybersecurity Forum

  - IESO led forum for Ontario market participants.

- Focusing on collaboration, development of best practice and sharing of cybersecurity related information.

- Taking place November 2013.

Additional Information

Ben Blakely

Team Lead Security & Enterprise Security Architect, IESO

ben.blakely@ieso.ca

905-855-6305