The five questions I am being asked by National Policy Makers and Utility CEOs; My Best Answers; And Where the Questions Don't Have Answers

The 7th Annual North American SCADA and Process Control Summit
January 27, 2012

Michael J. Assante
NBISE
Questions from CEOs & Executives
Q: Where do the cyber risks that I should be most concerned with reside in my enterprise?

“To my mind, coordinated cyber attack is a significant reliability threat facing the electricity industry ... Coordinated cyber security threats are real and preparing for them needs to be built into our planning, into our design and into our daily operation.”

– Electric Sector CEO, 2010
Cyber Risk are in the Business

**Generation**
- Automated Generation Control
- Plant Systems (PCS/Safety/Historian)
- Remote Access (3rd Parties/Internal)
- Market Systems
- Network Connections

**Transmission**
- System Control Center SCADA EMS
- Substation (Control & DA/Protection)
- Phasors, Data Concentrators, Gateways
- Remote Access (3rd Parties/Engineering)

**Distribution**
- Advanced Metering
- System Control Center SCADA DMS
- Substation (Control & DA/Protection)
- Distribution Automation (Remote Disconnect)
- Phasors, Data Concentrators, Gateways
- Outage Management Systems
- Remote Access (3rd Parties/Engineering)
- DOE ARRA Security Plan

You must address in your Operational Technology environments
Secure It - - How About Understand It?

- NISTIR 7628 “Spaghetti” Diagram: Logical Reference Model

"Any intelligent fool can make things bigger, more complex, and more violent. It takes a touch of genius -- and a lot of courage -- to move in the opposite direction." - Albert Einstein
Your people should worry about:

- The potential for an intelligent cyber attacker to exploit a common vulnerability that impacts many assets at once, and from a distance
  - Common or single point(s) of failure
  - Universal points for commands/action
  - Remote access
  - Data & network concentrations
    - Convergence of safety and control systems
  - Inherent trust in the system and between components
  - Growing system complexity
    - Develop flexible models and architectures
    - Reverse the convergence of safety/protection and control systems
  - Remove silos and integrate cybersecurity into operations
    - Training operators to observe and consider
  - Develop team responses with shared expertise
Q: If my organization performs well in complying with the current version of NERC’s CIP Standards are we okay?
My response

You sure you want me to answer that one?
Standards as a Tool to Manage Risk

- Standards are a good tool to manage risk when it is either well-bounded and understood or when the standard simply codifies well-honed industry practices that are proven to be successful.
- Mandatory cyber standards fail both of these conditions, mainly because advanced cyber threats are not probabilistic in nature, but represent a co-adaptive risk.
- Regulation, although necessary, should be re-evaluated and designed to emphasize learning, share responsibility across the technology chain, enable the development of greater technical capabilities through more qualified staff, and discourage the creation of a predictable and static defense.
Q: Where am I underinvested to manage the risk associated with cyber threats?

My responding question - Q: Are you asking about security or are you including compliance violations in your risk calculation?
My Response

- This is an important question

- Cybersecurity is like an arms race – there is no silver bullet investment to be made

- You must make sufficient technology investment to gain necessary coverage and penetration into your IT & OT systems…….“Necessary but not sufficient”

- Your most important investments should be in your people
  - Developing winning strategies
  - Developing the right skills
The Electronic Arms Race of Cyber Security

Opportunity
Theft
Hackers learn to eavesdrop

Hackers compromise routers to bypass walls
Simple packet injection attacks

Man-in-the-middle attacks
Crack passwords
Use “social engineering”

Coordinated distributed denial-of-service

Coordinated distributed denial-of-service

Stuxnet
NextGen Attack

Problem with “Incrementalism”

Most Likely

Trivial
Minimum effort
Moderate attacks
Targeted attacks

In Development

Worst Case

limit physical access
Managers use a single password for all routers
Audit and fix bad TCP/IP stacks
Define strong passwords
Implement awareness program
Implement firewalls
Blackholing

Security

Adversary

Adversary capability
Security capability

“Window of Susceptibility”

“It Never Ends”
I like to tell a story

- Take them back to a decisive contest
  - Involved the best technology of the day

The year was 1805 and the contestants were the British Fleet versus the Franco-Spanish Fleet
The contestants invested in very different things

The French and Spanish....

Possessed the largest & most gunned ships + Brought more ships than the British = Technological advantage

33 Ships of the Line - Largest ships had 136 guns on 4 decks

25 Ships of the Line - Largest ships had 100 guns on 3 decks

....invested heavily in the best technology of the day
The contestants invested in very different things

The British….

Well practiced gunners
+ Able bodied commander
= Winning Strategy

….invested heavily in skills and strategy
Questions from Policy Makers
Q: What needs to be protected from cyber threats in the power system?
That is the right question!
“The Largest Machines in the World”
My Response

- Prioritization is critical – but can be dangerous
- The challenge comes in answering the following questions:
  - Are we protecting the correct assets properly? (Where properly is some level of “adequacy” determined by policymakers and correct assets is a group that if harmed would result in damage that justifies the government’s interest.)
  - Who pays for the necessary investment to mitigate the risk?
    - Unfunded mandates can result in significant impacts to individual businesses, industries, and society (i.e. higher electricity prices)
    - Funded mandates require public trade-offs
    - Compliance does not equate to enhanced security
  - How does the public & private partnership effectively mitigate co-adaptive risk?
Q: Will industry be able to achieve progress without government action or oversight?
Response

- Threats of the 21st century are unlike those of the past
  - Government’s traditional role as protector of the people does not fully extend into the cyber realm
  - Responsibility, now more than ever, lies with private sector to secure assets from new “acts of war”

- Private sector entities have not made sufficient progress (nor has government) to warrant leaving this national issue to the potential target organization

- Oversight can motivate action but you must be very careful as to what you are motivating!
The five questions I am being asked by National Policy Makers and Utility CEOs; My Best Answers; And Where the Questions Don't Have Answers

QUESTIONS?

The 7th Annual North American SCADA and Process Control Summit
January 27, 2012

Michael J. Assante
208-557-8026
Michael.assante@nbise.org