



***Using the
Threat-to-Consequence Process
to Reduce Risk of Cyber Attacks
on Critical Infrastructures***

Laurence R. (Laurie) Phillips
Sandia National Laboratories

Overview

- **Goals**
- **30,000 foot view of the workshop**
- **Two Fundamental Questions**
- **We need your help**
- **A Holistic Approach to Risk**
- **Stakeholder Goals from the 2006 *Roadmap***
- **Our risk-mitigation strategy**
- **The components of risk**
- **Threat-to-Consequence Risk Analysis Framework**
- **Collaborating to Reduce Risk**

Goal of the NSTB Program and of this Workshop

Reduce Cyber Risk

Reduce the risk of
major consequence
due to cyber attack
on U.S. critical infrastructure

**Today we'll address getting
the information needed to
make risk-mitigation
decisions based on a
fictional scenario**

**In the future
we want to focus on
genuine issues**

The fundamental critical infrastructure risk questions:

- How does it affect the asset owner ?
- How does it affect the nation?

Sandia's NSTB Project provides information that asset owners and the government need to make informed decisions ...

But ...

We Need Your Help

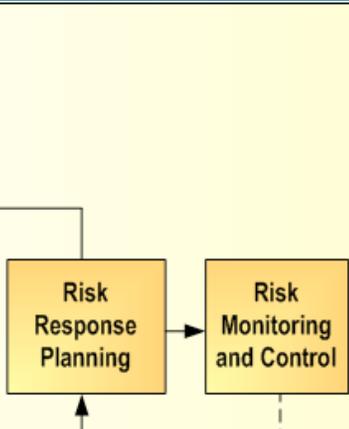
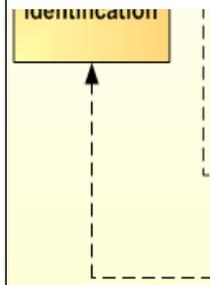
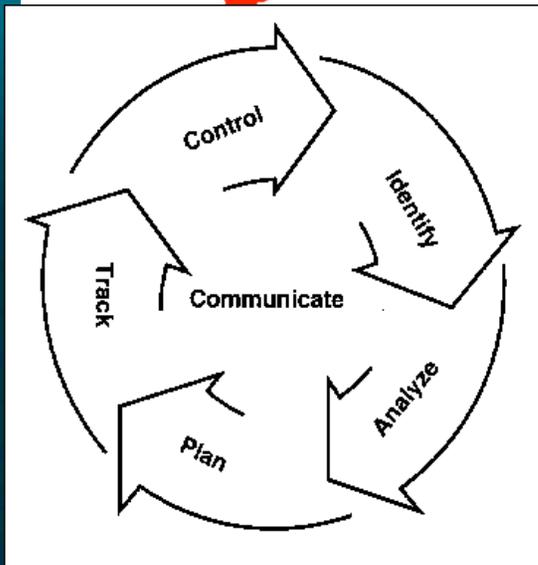
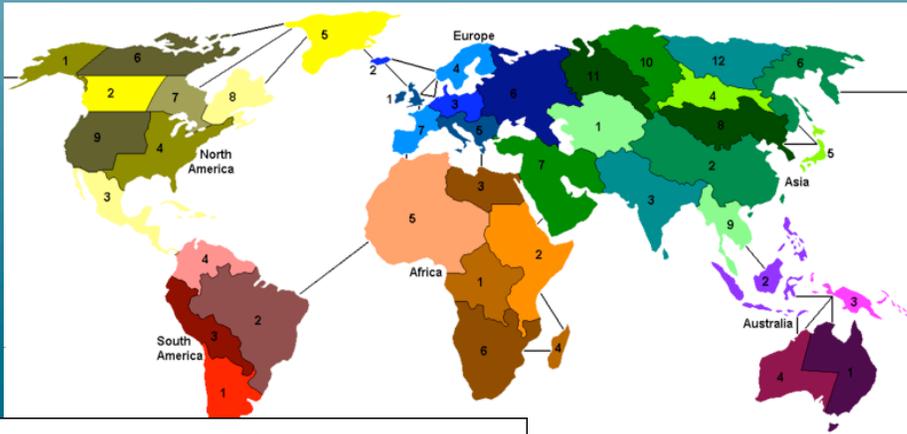
- We are tackling the job of assessing cyber risk
- We have a national* perspective
- We also need a realistic view of the infrastructure
 - We don't operate the infrastructure
 - We need to engage those who do
- Today you'll see what we're doing and how you can get involved

* national issues are *large and cut across sectors and regions*

An Holistic Risk Management Process

- In a nutshell:
 - Evaluate the cyber risk spectrum
 - Address the greater risks
 - Continue until residual risk is acceptable
- You should consider the whole risk spectrum
 - It's a big job—and if that's all you do, you're only *studying* risk
 - Constant flow of new technology means you'll never finish
 - This is one you hope somebody else will do (it's a national issue)
 - But there are benefits:
 - More bang for the cyber-security buck
 - Strategies can be more broadly effective
 - You can defend your actions: “Our approach provides the greatest reduction in risk for this level of effort.”

So ... Risk?



What matters is whether risk is:

high

YOU NEED TO FIX THIS RIGHT NOW

medium

YOU NEED TO FIX THIS BUT IT CAN WAIT

low

YOU CAN WORRY ABOUT THIS LATER

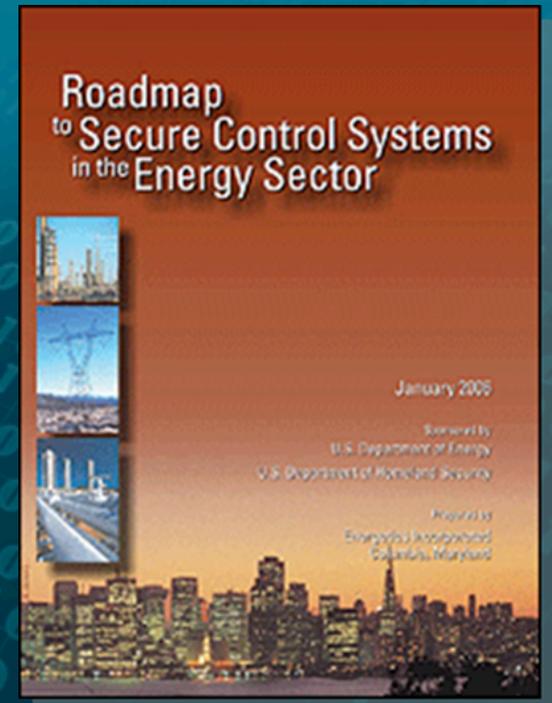
Roadmap Goals

supported by the NSTB program
and this workshop

The following risk analysis
elements are called for in

Roadmap to Secure Control Systems in the Energy Sector :

- **Cyber attack and response simulators**
- **Balance threat, vulnerability, and consequence**
- **Risk assessment tools**
 - Vulnerability assessment method
 - Framework for prioritizing control measures
 - Business case
- **An information-sharing environment**



January 2006

What's missing?

**A framework
unifying these
Roadmap elements**

A Unifying Concept: The Threat-to-Consequence Framework



**Today we'll address each
component**

A Unifying Concept: The Threat-to-Consequence Framework



**Today we'll address each
component**

**... and we'll see how everything
fits together to provide insight
into infrastructure cyber risk**

Our Approach to Managing Infrastructure Risk

A Definition of Risk:

Bear with me ...

we need a list of the things that make up risk.

$$R = T * V * C$$

- T = Threat** = likelihood a threat will attack
- V = Vulnerability** = probability a given threat's attack will succeed vs. a given vulnerability
- C = Consequence** = defender's cost due to successful attack
- It is helpful to consider:
 - Effect (part of V): What cyber effects are caused by exploitation?
 - Impact (part of C): What happens to the infrastructure itself?

The Threat-to-Consequence (T-to-C) Framework embodies the risk equation



- T {
- **Possible threats**: Who might do us harm?
 - **Plausible threats**: Which ones should I care about?
- V {
- **Effects**: What are the cyber effects when the vulnerability is exploited?
- C {
- **Impact**: What's the infrastructure damage?
 - **Consequence**: What's the societal cost?

For example,
here's a
high-medium-low approach
to
EFFECT & IMPACT

Effect & Impact Analysis

How hard is it to achieve the result?

Effect characterization elements			
cyber operation	complex	multi-step	simple
hardware specification	detailed	relevant	broad
component count	high	moderate	low
component variety	high	moderate	low
coordination	complicated	some	none
timing	precise	relevant	irrelevant
attack plan complexity	high	moderate	low
capability maturity	unknown	tried	understood

green = less concern

because the result is harder to achieve

red = more concern

because the result is easier to achieve

- An effect with lots of green is hard(er) to achieve, so it's:
- less likely to work correctly
 - less appealing to an adversary
 - less likely to be deployed

What about threat, regional impact, etc.?

- Without going into detail (we'll see more later), the rest of the T-to-C framework is similarly analyzed
- And the results combined into a profile for a given:
 - Threat
 - Vulnerability
 - Effect
 - Scenario
 - Regulation
 - ... (other possibilities)
- You'll see this approach applied over the course of the workshop, and we'll present a summary of overall risk at the end of the day

The T-to-C framework allows critical infrastructure stakeholders to gain value from our work



- Our goal is to analyze a catalogue of scenarios that span existing vulnerabilities
- New threats, vulnerabilities, and scenarios can be compared with these to find out how much risk they represent
- For issues that represent substantial risk:
 - Further analysis with more complex tools (as you'll see today)
 - Mitigation analysis and implementation

Collaborating to Reduce Risk

- **Declare a topic of interest**

You can provide this

- **Develop a scenario that covers the topic**
- **Assess risk**
- **Make a decision:**
How much effort should be put into reducing this risk?
- **Choose the mitigation strategy that reduces risk the most**

*We can help here
(today's workshop shows
our approach)*

What's meant by "You"?

(as in "You can provide this")

- **We welcome collaboration with utilities**
- **We invite:**
 - Individual owner-operators
 - Ad-hoc groups of owner-operators
 - Sector associations and boards
 - Industry associations
 - Government
- **We have a national focus, but smaller stakeholders may exemplify national issues**

Contact us with topics of interest

- **POC: Bob Pollock**
 - rdpollo@sandia.gov
 - (505) 844-4442

Questions?

- **We have experience and mechanisms that allow us to work with both governmental and private industries.**
- **Where there's a will, we'll find a way**