National Infrastructure Advisory Council (NIAC)

The Insider Threat to Critical Infrastructures

Thomas Noonan
General Manager
IBM Internet Security Systems

Edmund Archuleta
General Manager
El Paso Water Utilities

Overview

- Objective
- Scope
- Phase I Preliminary Findings
  - Defining the Insider Threat to Critical Infrastructures
  - Analysis of the Dynamics and Scope
  - Defining the obstacles to addressing the insider threat
  - Analysis of the impact of Globalization on the Insider Threat
- Next steps
- Questions

Objective

- To define the insider threat to critical infrastructures, including dynamics involved, obstacles to mitigation, and the effect of globalization.
- The second phase of the study will focus on legal, procedural, and policy barriers for private sector infrastructure operator employee screening efforts.
- Completion of the study may produce potential recommendations for improving operators' ability to address the insider threat to critical infrastructures, and seek to provide guidance on a clear legal environment for operators in dealing with potentially hostile insiders.

Scope

- Scope of the study (as outlined in the January 16 letter from Secretary Chertoff):
  - ✓ Define the "insider threat" physical and cyber, including potential consequences, economic or otherwise
  - ✓ Analyze the dynamics and scope of the insider threat including critical infrastructure vulnerabilities
  - ✓ Analyze the potential impact of globalization on the critical infrastructure marketplace and insider issues
  - ✓ Identify/define the obstacles to addressing the insider threat
  - ✦ Identify issues, potential problems, and consequences associated with screening employees
  - ✦ Identify legal, policy, and procedural barriers aspects of the issue, as well as any potential obstacles, from the perspective of the owners and operators
  - ✦ Identify and make policy recommendations on potential remedies for addressing the insider threat (up to and including potential legislation)

Preliminary Findings: Defining the Insider Threat to Critical Infrastructures

The January 16 letter to the NIAC stated**:** Define the "insider threat" for physical, cyber, and combined and include analysis economic consequences.

- *Definition:* the Insider Threat to critical infrastructure is an individual with the access and/or inside knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with the intent to cause harm
- Critical Infrastructure-level threats affect critical infrastructure services delivery, the national economic back-bone, or public health and safety

Preliminary Findings: Analysis of Dynamics and Scope of the Insider Threat

Scope:

- Focusing on Critical infrastructure level threats – those that affect CI services delivery, the economic back-bone, or public health/safety
- Variation among sectors on maturity and awareness
- Potential actors include: disgruntled employees, economic espionage, and infiltration

Dynamics:

- Lack of hard data for universal definition
- Globalization is escalating exposure and costs of these threats
- Technology and network risks rapidly escalating
- Complacency and denial are key components

Preliminary Findings: Defining the Obstacles to Addressing the Insider Threat

- Difficult to define due to lack of hard data
- Education and awareness is possible; needed cultural change is more difficult
  - Investment in structured programs and risk management
  - Corporate culture of trust runs counter to prevention programs
  - Workforce relations can complicate targeted efforts to address insider threats
- Use of background checks varies among sectors and are not universally accepted - regulation is controversial as a solution
- Multiple legal environments complicate Insider Threat mitigation strategies
  - Federal, state, local and multinational

Preliminary Findings: Analysis of the impact of Globalization

- Introducing enormous macroeconomic forces to the marketplace
  - Pushing large scale changes and introducing new threats for critical infrastructure operators
- Expanding IT networks and increasing risk
- Expanding the group of *insiders* - populations are less verifiable, and may be less reliable
- Varying legal environments among different countries
- Global supply chain used by infrastructure operators is increasing potential for expanded insider threats or *agents*

Next Steps

- Complete *Phase I* research
- Outline all secondary issues and their impact
- Draft recommendations
- Publish coordinating draft of report
- Begin *Phase II* research

Questions?