Understanding Critical Infrastructure Cybersecurity

Introduction to Concepts, Language, Policy
About me…

• Jack Whitsitt | http://twitter.com/sintixerr | jack@energysec.org

• Broad Background
  – Lived in a little hacker compound as a kid
  – Started with Open Source development (Rubicon03)
  – MSSP:IDS, Data Viz, Anomaly Detection Designer
  – Enterprise Security Architecture
  – ICS-CERT (INL)
  – Past Federal Employee with Nationally-scoped cyber responsibilities

• Now
  – Non-profit Community Builder & Facilitator
  – Focus on Electric Sector
  – Frameworks Frameworks Frameworks
Overview

Start with Language

– Defining “Cybersecurity”
– Mission Landscape Part I: Theory
– Defining “Critical Infrastructure”

Follow with Details

– Mission Landscape Part II: Practice
– Critical Infrastructure Security Nuance
– Consequences, Motivations, and the State of the World
What is “Cybersecurity”? 
Why define cybersecurity?

• Everyone has a different perspective:
  – Information Security
  – Data Security
  – Computer Security
  – Control Systems Security
  – Network Security
  – Information Risk Management
  – Etc.

Even debating whether there’s a “space” between cyber and security
Identify Most Common Users:

- “Executives”
- “The Government”
- “The media”
- “Uncool lawyers”
- Regulators and Regulation Auditors
- Standards bodies
- Money, investment, and resource managers

Hmm…
Identify Core User Activities

• Communications
• Meetings
• Marketing & Sales
• Policy Development
• Frameworks
• Partnerships
• Facilitation
• Deferring to Non-Expert Authority
• Teaching
Define by Ontological Value

• There is a larger environment beyond technology that has to be hospitable to progress: Aware of the issues, able to receive and translate information, mature enough to pivot toward sustainable change.
• The most common users of the word “cyber-*” define and manage this larger environment and context
• Their activities (which synthesize multiple disciplines - both technical and non-technical) can sustainably improve (or inhibit) the *environment* for other more technical or tactical security activities, particularly at an industry or national scale and in the context of government laws, policies, mandates, and regulations
• This can said to be the practice of “Cybersecurity”
• Without “Cybersecurity”, the other more technical disciplines – “information security”, “data security”, “computer security”, “pen-testing”, “IDS monitoring”, “reversing”, whatever – lack the context required to make them most productive and pertinent
Applying the Team: First Find Natural Parentheticals

**Boss Bob**

I want to steal hazardous materials!

**Cyber Planning Bob**

Ok, we’ll attack Traffic Light Controls and make trucks stop!

**Hacker Bob**

Metasploit to the rescue!

**EVIL**

**GOOD!**

**CEO Jim**

I want to keep making $123 a day!

**IT Architect Jim**

Let’s make sure IT enables $123/day

**Security Jim**

IDS to the Rescue!

“Technology”
Refine to a Protocol Stack

- **National Security Assurance**
  - Assure Nation will continue; Diplomacy; Military

- **Business Environment**
  - Define Common Business Outcome Goals for Cyber security; Describe Environment; Create Common Lexicon

- **Capability Management**
  - Evaluate capabilities against organizational goals; prioritize resources and investments; adjust capabilities in response to ops data

- **Control Management**
  - Evaluate conceptual application of best practices, standards,

- **Operations & Testing**
  - Compare conceptual control placement to actual configurations and threats
Refine to a Protocol Stack

- National Security Assurance
  - Assure Nation with cybersecurity; Military

- Business Environment
  - Define Common Business Outcome
    Goals for Cyber security; Describe Environment; Create Common Lexicon

- Capability Management
  - Evaluate capabilities against organizational goals; prioritize resources and investments; adjust capabilities in response to data

- Control Management
  - Evaluate conceptual application of best practices across a number of best practices

- Operations & Testing
  - Compare conceptual control placement to actual configurations and threats
Mission Landscape Part I: Theory
Four Mission Overlap Problems (At Least)

- Protection vs. Assurance
  - High consequence, need “Assurance” that “Protection” is happening…but by Whom? How? Metrics?
  - Lack of Assurance leads to Excess Protection
  - Both government and industry have clear “assurance” needs

- Risks to vs. Risks From
  - Managing tactical risk to computers themselves
  - Managing the long term, strategic risk from computers

- Offense vs. Defense
  - Since “Cybersecurity” is often not defined, roles confused
  - NSA, DHS for instance

- Geographic Force Arrangement
  - This is interesting…
Force Mission Overlap I: Customers

- Citizens
- Individual Businesses
- Industries
- National Infrastructure
- Government infrastructure
- National Cohesion
Force Mission Overlap II: Vectors

• Contestable Threat Vectors (CTV):
  – Provide defendable space between “bad guys” and targets
  – Imply that there is a space that is *not* the target that must be traversed beforehand
  – (Just my term)

• Historically…
  – Earth
  – Air
  – Water
  – Space (for some value of historically)
Government “Security” apparatus responsibilities heavily influenced by geography

- The military protects national sovereignty outside the U.S.
- DHS protects national cohesion; operates on U.S. as a whole
- FBI specific aspects of internal U.S. interests
- State & Local government organizations
Force Mission Overlap IV: Along Came A Cyber

- "Cyberspace" comes along; screws things up
  - Cyber Assets: Targets AND part of a CTV
  - "Customers of Protection" now own a CTV
  - Geographic Protection Schemes break
  - Opaque by Default

- But can have consequences in other CTVs
  - So we can’t ignore old physical policy mechanisms
  - "National Guard" example
Getting Work Done Despite Everything

• Levers
  – Independent Action
  – Industry Action
  – Congress & Lawmaking
  – Courts
  – White House & Executive Branch
  – Military

Critical Infrastructure Focus is (mostly) “WH/Executive” + Industry

Courts take awhile, Congress is an inflexible hammer, military suffers from mission problems
Getting Work Done Despite Everything

• Why not just industry or independent action?
  – We (security practitioners) have made a lot of noise (as did, unfortunately, other countries)
  – Lack of government assurance from industry means they will act
    • Remind me to talk about this later 😊
  – If the government is acting, it is better to do it in coordination with industry than not
  – Also, it’s not as if industry is succeeding by itself
    • Also remind me to come back to this 😊

• So what is the “White House/Executive/Industry Engagement”?
  – Glad you asked!
Wait! What IS “Critical Infrastructure”? 

• Formal and informal definitions  
  – Average “on the street” definition can be anything  
  – Formal definitions actually exist in policy and law (we’ll get there)  

• Concept: Ultimate Consequence Owner  
  – There are many “critical” industries and groups in the U.S.  
  – Some “critical” because of the immediate, direct outcomes of failure  
  – Some “critical” because of their impact on the former  
  – Formal “Critical Infrastructure” designations (mostly) revolve around the former type
Mission Landscape Part I: Practice
Primary Documents (Until 02/2013): HSPD-7/NIPP

• “Homeland Security Presidential Directive-7”
  – Bush. Builds on earlier directive from Clinton
  – Assigns Critical Infrastructure Protection to DHS

• National Infrastructure Protection Plan (NIPP)
  – DHS Plan for Implementation of HSPD-7

• “All” Critical Infrastructure, not just Cyber
  – Most of the people traditionally involved are *not* cyber
  – This isn’t entirely wrong, but causes public disconnect

• They do require cyber-specific actions from DHS
  – Confusing. One of the reasons for the EO

"It is the policy of the United States to enhance the protection of our Nation's critical infrastructure and key resources against terrorist acts that could:

- Cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction;
- Impair Federal departments and agencies' abilities to perform essential missions, or to ensure the public's health and safety;
- Undermine State and local government capacities to maintain order and to deliver minimum essential public services;
- Damage the private sector's capability to ensure the orderly functioning of the economy and delivery of essential services;
- Have a negative effect on the economy through the cascading disruption of other critical infrastructure and key resources; or
- Undermine the public's morale and confidence in our national economic and political institutions."
HSPD-7 Policy Statement

RealSpeak Summary:
The U.S. will protect the infrastructure supporting National Cohesion” in Partnership with Industry

Experience says:
• “Protect” doesn’t have to be active
• “Protect” really means “Assure Security”
• “Assurance” starts with measuring and only continues to protecting *if* the measurements fail
Primary HSPD-7/NIPP Goals

- Identify Critical Infrastructure
- Prioritize Infrastructure
- Protect
- Report on Progress

This means: Create specific plans to, in voluntary cooperation with industry, implement the NIPP Risk Management Lifecycle and report annually.
Dividing Ownership

- US Government (HSPD-7/NIPP) splits Critical Infrastructure responsibilities into 16 “Sectors”
- Each “Sector” is assigned a “Sector Specific Agency” (“SSA”)
- Assignments are done at a Department level
  - Some departments assign SSA responsibilities to sub-organizations (e.g. DHS assigning Transportation to TSA)

<table>
<thead>
<tr>
<th>Chemical: DHS</th>
<th>Financial Services: Treasury</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commercial Facilities: DHS</td>
<td>Food and Agriculture:Agg/HHS</td>
</tr>
<tr>
<td>Communications: DHS</td>
<td>Government Facilities: DHS/GSA</td>
</tr>
<tr>
<td>Critical Manufacturing: DHS</td>
<td>Healthcare and Public Health: HHS</td>
</tr>
<tr>
<td>Dams: DHS</td>
<td>Information Technology: DHS</td>
</tr>
<tr>
<td>Defense Industrial Base: DOD</td>
<td>Nuclear: DHS</td>
</tr>
<tr>
<td>Emergency Services: DHS</td>
<td>Transportation Systems: TSA/DOT</td>
</tr>
<tr>
<td>Energy: DOE</td>
<td>Water and Wastewater Systems: EPA</td>
</tr>
<tr>
<td><strong>Sector Specific Agency Responsibilities</strong></td>
<td></td>
</tr>
<tr>
<td>------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Encourage organizations</strong> with information to share with those who need it and <strong>encourage development</strong> of <strong>sector information sharing programs</strong> and mechanisms</td>
<td></td>
</tr>
<tr>
<td><strong>Promote education</strong>, training, and awareness within the sector in coordination with other government and private sector partners</td>
<td></td>
</tr>
<tr>
<td><strong>Identify, prioritize, coordinate</strong> federal CCIP activities in sector</td>
<td></td>
</tr>
<tr>
<td><strong>Appraise congress</strong> of sector's current status and progress in <strong>reducing risk</strong> and <strong>implementing the NIPP</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Increase integration</strong> of cyber security efforts with other all hazards protection and response programs</td>
<td></td>
</tr>
<tr>
<td><strong>Develop and implement sector risk management program</strong> and framework and use to <strong>determine risk priorities of sector</strong> and <strong>coordinate</strong> risk assessment and management <strong>programs</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Support</strong> Ad-Hoc DHS data calls</td>
<td></td>
</tr>
<tr>
<td><strong>Promote cyber awareness</strong> of owners and operators and <strong>program level guidance</strong> for CIKR protection</td>
<td></td>
</tr>
</tbody>
</table>
“Public/Private Partnership”

• Formal Term, Formal Constructs
  – Used in many contexts
• Foundation of Critical Infrastructure Protection in the US
• “Voluntary”, “Public”
  – (Limited? Trust issues)
• Alternative is/has been Regulation
• “Weight of Government Burnout” problems
• This is important
The primary organizational structure for coordinating critical infrastructure efforts and activities.
Facilitates integration of all partners into planning & ops activities
Ensure a collaborative approach to critical infrastructure protection.
The SCCs and corresponding GCCs work in tandem to create a coordinated national framework for Critical Infrastructure protection and resiliency within and across sectors.
Sector Coordinating Councils (SCC’s)

• The principal entities for CIKR owners and operators within a sector to coordinate with the government
• Include a broad base of owners, operators, associations, and other entities
• Principal private sector policy coordination and planning entities
• Participate in planning efforts related to reporting for the NIPP
• For information sharing and response, often rely on ISACs and other non-SSA entities
• **Problem:** This is probably the first time you’re hearing this (also: industry vs citizens)
Government Coordinating Councils (GCC’s)

• The government counterpart for each SCC to enable interagency and cross-jurisdictional coordination within a sector
• Includes representatives from various levels of government (Federal, State, local, or tribal) as appropriate
• Co-chaired by a representative from the designated SSA and DHS IP (This causes some issues)
• Coordinates with and supports the efforts of the SCC to plan, implement, and execute the Nation’s CIKR protection mission.
• Provides interagency strategic communications, discussion, and coordination at the sector level
• Participates in NIPP planning efforts
What is “CIPAC”? 

• DHS Construct: Critical Infrastructure Partnership Advisory Council 
• Provides a legal framework for SCC and GCC members to engage in joint CIKR protection-related activities 
• Operational mechanism of National Infrastructure Protection Plan (NIPP) 
• Provides membership to agencies across all levels of government and the private sector, including membership representing almost 50 percent of the Gross National Product of the United States. 
• Allows members of Sector Coordinating Councils (SCC) and Government Coordinating Councils (GCC) to engage in cross-Sector, cross-government coordination. 
• Key activities of the CIPAC include information sharing, national planning, and program implementation
CIPAC: Good & Bad

• Good
  – No FACA, Not owned by government
  – Managed Engagement
  – **Must** Have SCC co-chair

• Bad
  – Control issues (SSA’s don’t always like it)
  – Trust Issues (Northwest Rail story)
CIPAC Examples

• Industrial Control Systems Joint Working Group (ICSJWG)
• Cross Sector Cyber Security Working Group (CSCSWG)
• Transportation Systems Sector Cybersecurity Working Group (TSSCWG)
What about technical security?

- NCCIC
- ICS-CERT
- CISCP
- NLE/Cyberstorm
- US-CERT
- ISACs
Aside: Government “Information Sharing”

- “Incident Response” organizations are often regarded as “Information Sharing” ones
  - Must not forget distinction
  - Missions may conflict and impact sharing
- FBI, Military, and the Intel Community also have potentially conflicting missions
- No Pot of Gold at the end of the Classification Rainbow
- Information often classified due to sources and means, not content
- Actionable REQUIRES bi-directional sharing
HSPD-7 & NIPP Environment

Sector Coordinating Councils (Industry)

- CIPAC
- CRADA/PCII

Public/Private Partnerships

Resource Coordination

Government Coordinating Councils

Fed to Fed

Government Cyber-Specific Operations

National Planning

Security Operations
New Policies

• Cyber Executive Order:
  – **Aimed at Gov, Not You: Mom reigning in kids**
  – Cyber was already supposed to have been being handled (as we’ve seen)
  – Attempts to rectify these barriers while keeping in tact most of the fundamental structures already in place.
  – **Heavy focus on “Harmonizing Cyber Efforts”** ← Awesome

• Presidential Policy Directive (PPD-21)
  – Not Cyber specific – update to HSPD-7
  – Important
Three strategic imperatives shall drive the Federal approach to strengthen critical infrastructure security and resilience:

1) Refine and clarify functional relationships across the Federal Government
   • Federal functions related to critical infrastructure security and resilience shall be clarified
   • There shall be two national critical infrastructure centers operated by DHS – one for physical infrastructure and another for cyber infrastructure.

2) Enable effective information exchange by identifying baseline data and systems requirements for the Federal Government; and
   • Enable efficient information exchange through the identification of requirements for data and information formats and accessibility, system interoperability, and redundant systems and alternate capabilities should there be a disruption in the primary systems.

3) Implement an integration and analysis function to inform planning and operations decisions regarding critical infrastructure.
   • Shall include the capability to collate, assess, and integrate vulnerability and consequence information with threat streams and hazard information
Whitehouse Cyber Executive Order

Main Thrusts:

– Improve Information Sharing
– Use business-function driven risk analysis to determine priorities
– Create a framework of standards for reducing risks from cyber security issues to critical infrastructure
– Engage industry to the greatest extent possible, and assure privacy and civil liberties are embedded in the entire process.
Executive Order: Section Analysis

1. – 3. Fluff
4. Cybersecurity Information Sharing
5. Privacy and Civil Liberties Protections
6. Consultative Process
7. Baseline Framework to Reduce Cyber Risk to Critical Infrastructure
8. Voluntary Critical Infrastructure Cybersecurity Program
9. Identification of Critical Infrastructure at Greatest Risk
10. Adoption of Framework (Read: Potential Regulation)
Critical Infrastructure Security Nuance
Control Systems Vulnerabilities

- Business Value Chains
  - Supply Chain
  - Support Models
- Control Systems
  - Culture: Engineering vs IT
  - Separation & Evolution: Connected physically, Culture slower
  - Technology: Fragility, “HMI”s
  - Testability and Visibility
- Lifecycles
  - Purchasing
  - Replaceability
- Scale
  - Imagine asking every critical company in the US to design and build every *car* it uses. Asking every critical company to do security guarantees quality/rate issues
Closing Thoughts:
Consequences, Motivations, and the State of the World
Consequences & Motivations

• “Can someone shut down the power grid?!?!?”
  – Maybe. We don’t know.
• “I don’t believe you. I think it’s impossible”
  – It doesn’t matter, if we don’t *know*
• “Of course it matters!”
  – Not if you want to influence behavior
• “What do you mean?”
  – …
Consequences & Motivations

• Can’t prove if a specific consequence possible (now)
  – Emergently complex
  – Technical, Cultural, Business considerations
• Other motivations realistic
  – Command Decision Making Delay
  – Blackmail (Bluffing or otherwise)
  – Tactical Aid to Blended Attacks
  – Misdirection/Sleight of Hand
  – Etc
• Those consequences are all possible
  – APT? Persistent access from well organized and funded threat groups capable of mounting multiple blended missions over time in environments with more unknown vulnerabilities than zero that we neither fully understand, nor manage, nor control.
State of the World

My opinion: There is a lot of work being done. So far, it hasn’t worked yet. Game theory says we should be stabilizing what we’re doing to get the most predictable results and then alter the underlying environment if we want *better* results. Our long term success or failure in critical infrastructure will depend on how well (or even if) we reconceptualize our environment and make it more hospitable to security. We’re moving in that direction, but it takes time and “above and beyond” effort. CISO’s aren’t, generally, on the hook to try and save the world.