National Cyber Incident Response - Architectural Concepts
Protection Imperatives

- Protection of critical infrastructures, including information infrastructures is a matter of national security, economy, public welfare, and safety
- A high percentage (85% in U.S.) of critical infrastructure assets and key resources are privately owned; and we can assume a larger percentage for information infrastructures
- National goals for the protection of critical infrastructures cannot be accomplished without strong public-private partnerships

“It is the policy of the United States to protect... the operation of the information systems for critical infrastructure, and thereby, help to protect the people, economy, essential human and government services, and the national security of the United States, and to ensure that any disruptions that occur are infrequent, of minimal duration, manageable, and cause the least damage possible.”

Executive Order on Critical Infrastructure Protection, 16 October, 2001

Protection Scope

10+ Critical Infrastructure Sectors (17 for the U.S.)
- Agriculture and Food
- Energy
- National Monuments & Icons
- Drinking Water
- Postal and Shipping
- Transportation systems
- Government Facilities
- Telecommunications
- Information Technology
- Defense Industrial Base
- Public Health and Health Care
- Banking and Finance
- Chemical
- Commercial Facilities
- Dams
- Emergency Services
- Nuclear reactors, materials, waste

Source: U.S. National Infrastructure Protection Plan, 2006
Critical Infrastructure / Key Resources

- **Agriculture and Food**
  - Farms
  - Food Processing Plants

- **Energy**
  - Power Plants
  - Production Sites

- **Transportation**
  - Railroad Tracks
  - Highway Bridges
  - Pipelines
  - Ports

- **Chemical Industry**
  - Chemical Plants

- **Postal and Shipping**
  - Delivery Sites

- **Water**
  - Reservoirs
  - Treatment Plants

- **Public Health**
  - Hospitals

- **Telecommunications**
  - Cable
  - Fiber

- **Banking and Finance**
  - FDIC institutions

- **Key Assets**
  - Nuclear Power Plants
  - Government facilities
  - Dams

Cyber Infrastructure

- **Internet**
  - Domain Name System
  - Web Hosting
  - IP Protocol
  - E-Mail

- **Hardware**
  - Servers
  - Desktops
  - Networking Equipment

- **Software**
  - Operating Systems
  - System Utilities
  - Program Applications

- **Control Systems**
  - SCADA
  - PCS
  - DCS

Protection Factors - Interdependency

National Response Planning Requirements - 1

• Identification of experts, critical assets / key resources, areas of responsibility, mutual countermeasures, best practices, and standards
• Coordination of vendor and service provider communities on technical and procedural solutions and remedies
• Coordination with other management frameworks (such as CIP programs, national emergency response plans, etc)
• Collaboration of government, nCSIRTs, intelligence services, and law enforcement
• Collaboration on planning, design, implementation, operation, and reconstitution processes with partners

National Response Planning Requirements - 2

• Identification of dependencies and interdependencies between critical infrastructure systems
• Identification of consequences of a critical infrastructure failure
• Identification of threats, risks, single points of failure, and major vulnerabilities
• Development of options for investment and other mitigation strategies
• Planning and testing using evaluations and scenarios, including natural disasters, criminal actions, and acts of sabotage/terrorism, which disrupt the supply of critical infrastructure services and test business continuity and other response plans
U.S. Environment of National Cyber Incident Response

U.S. Cyber Incident Planning Communities

- Federal Incident Response Community
  - DHS - National Cyber Security Division
  - Law Enforcement / Intelligence
  - Department of Defense
- Information Sharing and Analysis Centers
- Sector Coordinating Councils
- Government Coordinating Council
- International Entities
National Response Framework

- Presents guiding principles that enable all response partners to prepare for and provide a unified national response to disasters and emergencies – from the smallest incident to the largest catastrophe.

- Supersedes NRP, December 2004.

NRF Quick Reference

Key Documents
- National Incident Management System (NIMS): Establishes a systematic approach for managing incidents nationwide.
- IFA, Report, and Incident Awareness: Provides concepts of operations, procedures, and structures for achieving response objectives.
- National Energy for Terrorism/ Security: Reflects the National Petroleum Council, which includes the National Planning Scenario.
- Response Partner Guides: Provides a ready reference of key roles and actions for local, tribal, state, Federal, and private-sector response partners.

Response Doctrine: Key Principles
- Engaged Partnership: Leaders at all levels must communicate and actively support engaged partnerships by developing shared goals and aligning capabilities so that no one is overwhelmed in times of crisis.
- Timely Response: Incidents must be managed at the lowest possible jurisdictional level and supported by additional capabilities when needed.
- Scalable, Flexible, and Adaptable Operational Capabilities: As incidents change in size, scope, and complexity, the response must adapt to meet requirements.
- Unity of Effort Through Unified Command: Effective unified command is indispensable to response activities and requires a clear understanding of the roles and responsibilities of each participating organization.
- Readiness To Act: Effective response requires readiness to act balanced with an understanding of risk. From individuals, households, and communities to local, tribal, State, and Federal governments, national response depends on the instinct and ability to act.
Federal Government Responsibilities under Framework:

- Providing indications and warning of potential threats, incidents, and attacks
- Information-sharing both inside and outside the government, including best practices, investigative information, coordination of incident response, and incident mitigation
- Analyzing cyber vulnerabilities, exploits, and attack methodologies
- Providing technical assistance
- Conducting investigations, forensics analysis, and prosecution
- Attributing the source of cyber attacks
- Defending against the attack
- Leading national-level recovery efforts

Organizations Involved:

- Interagency Incident Management Group (IIMG)
- National Cyber Response Coordination Group (NCRCG)
- U.S. Computer Emergency Readiness Team (US-CERT)
- Intelligence Community – Incident Response Center (IC-IRC)
- Department of Defense (DOD)

Supporting Agencies:

- Department of Homeland Security
- Department of Justice
- National Security Council
U.S. National Response Authorizations

- Homeland Security Presidential Directive-7 (HSPD-7)
- Federal Information Security Management Act (FISMA)
- Section 706, Communications Act of 1934, as amended (47 U.S.C. 606)
- The Defense Production Act of 1950, as amended
- National Security Act of 1947, as amended
- Executive Order 12333: United States Intelligence Activities, as amended
- National Strategy to Secure Cyberspace

Information Sharing & Analysis Programs

- ISACCOUNCIL.ORG
- SC ISAC
- PT-ISAC
- ISAC
- WaterISAC
- NERC
- ST-ISAC
- Emergency Management and Response - Information Sharing and Analysis Center (EMR-ISAC)
- InfraGard
- Real Estate ISAC
- FASCC
- CERT
- Software Engineering Institute
- Carnegie Mellon
US-CERT Overview

Strategic Operations
- Watch, Warning, and Incident Response
- Government Forum of Incident Response Security Teams (GFIRST)
- Chief Information Security Officers (CISO) Forum
- Computer Network Defense Service Provider (CNDSP) Accreditation Program

Federal Situational Awareness
National Cyber Alert System

LESSONS LEARNED
Use a Roadmap – ITU Example

I. National Strategy
- Create awareness at national policy level about cybersecurity and the need for national action and international cooperation.
- Develop a national strategy to enhance cybersecurity to reduce the risks and effects of cyber disruptions.
- Participate in international efforts for the prevention of, preparation for, protection from, response to, and recovery from incidents.

II. Government-Industry Collaboration
- Develop government-industry collaborations that work to effectively manage cybersecurity risk and to protect cyberspace.
- Provide a mechanism for bringing a variety of perspectives, equities, and knowledge together to reach consensus and move forward together to enhance security.

III. Deterring Cybercrime
- Enact and enforce a comprehensive set of laws relating to cybersecurity consistent with the provisions of the Convention on Cybercrime (2001).

IV. Incident Management Capabilities
- Develop a coordinated national cyberspace security response system to prevent, detect, deter, respond to and recover from cyber incidents.
- Establish a focal point for managing cyber incidents that bring together critical elements from government (including law enforcement) and essential elements from infrastructure operators and vendors to reduce both the risk and severity of incidents.
- Participate in watch, warning and incident response information sharing mechanisms.
- Develop, test and exercise emergency response plans, procedures, and protocols to ensure that government and non-government collaborators can build trust and coordinate effectively in a crisis.

V. Culture of Cybersecurity
- Promote a national Culture of Security consistent with UNGA Resolutions 57/239, Creation of a global culture of cybersecurity, and 58/199, Creation of a global culture of cybersecurity and the protection of critical information infrastructures.

“For a nation seeking to enhance cybersecurity and secure its critical information infrastructure, a first step is to establish cybersecurity as national policy.”

Understand National Strategy Impediments

Goal Orientation:
- Cybersecurity, business continuity, and ICT operations support critical information infrastructure protection (i.e., provide elements of resiliency) but are often performed independent of one another

Problem Recognition:
- The field of cybersecurity and CIIP tends to be focused on technical not managerial solutions; true process improvement elusive

Preparation:
- Nation’s have false sense of preparedness; only tested during disruptive events

Process:
- Codes of practice are numerous; however practice effectiveness is rarely measured

Measurement:
- There are few reliable benchmarks for determining an nation’s capability for protecting critical information infrastructures
Use Measurement & Metrics

Understand the Policy Framework
Utilize Policy Coordination Partnerships

Understand Supporting Success Factors

- Committed resources
  - Budget/People/Time
- Situational and security awareness
- Trained, Skilled, and Educated Partners and Principals
  - Design and conduct operational exercises
- Established communication channels (Public-Private Partnership)
- Developed risk criteria
- Established mitigation procedures
- Hardened information infrastructures
Understand CI Sector / Segment Perspectives

Use Modeling and Simulation

- Geospatial / Geopolitical
- Mission Critical Analysis
- Assurance Cases
- Dependent / Interdependent Risk Perspectives (CIIP)
- System Dynamics Modeling
National Level Exercise (NLE) - Objectives

- Exercise the national cyber incident response community with a focus on:
  - Interagency coordination under the Cyber Annex to the National Response Plan:
    - Interagency Incident Management Group (IIMG)
    - National Cyber Response Coordination Group (NCRCG)
  - Intergovernmental coordination and incident response:
    - Domestic: State – Federal
    - International: Australia, Canada, NZ, UK & US
  - Identification and improvement of public-private collaboration, procedures and processes
  - Identification of policies/issuses that affect cyber response & recovery
  - Identification of critical information sharing paths and mechanisms
- Raise awareness of the economic and national security impacts associated with a significant cyber incident

NLE Player Universe

An N^2 Problem
NLE - Lessons Learned – 1

- Correlation of multiple incidents is challenging at all levels:
  - Within enterprises / organizations
  - Across critical infrastructure sectors
  - Between states, federal agencies and countries
  - Bridging public – private sector divide
- Communication provides the foundation for response
  - Processes and procedures must address communication protocols, means and methods
- Collaboration on vulnerabilities is rapidly becoming required
  - Reliance on information systems for situational awareness, process controls and communications means that infrastructures cannot operate in a vacuum
- Coordination of response is time critical
  - Cross-sector touch points, key organizations, and SOPs must be worked out in advance
  - Coordination between public-private sectors must include well articulated roles and responsibilities

NLE - Lessons Learned – 2

- Strategic Communications / Public Messaging
  - Critical part of government response that should be coordinated with partners at all levels
- Policy Coordination
  - Senior leadership / interagency bodies should develop more structured communication paths with international counterparts
  - Strategic situational awareness picture cannot be built from a wholly federal or domestic perspective in the cyber realm
- Operational Cooperation
  - True situational awareness will always include an external component
  - Initial efforts at international cooperation during NLE provided concrete insights into of near term development of way ahead for ops/tech info sharing
  - Communication paths, methods, means and protocols must be solidified in advance of crisis/incident response
    - Who do I call? When do I call? How do I call them?
    - Secure and assured communications are critical in order to share sensitive information
  - Cooperation must include ability to link into or share info in all streams: e.g., Cyber, Physical, LE, Intelligence
Use International Resources

  • Available at: http://www.itu.int/ITU-D/cyb/

2007 Report on Policies to Protect the Critical Information Infrastructure (Australia, Canada, Japan, Korea, The Netherlands, United Kingdom, United States)
  • Available at: www.oecd.org/sti/security-privacy

International CIIP Handbook 2006:
  • Volume I: An Inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies
  • Volume II: Analyzing Issues, Challenges, and Prospects
  • Available at: http://www.crn.ethz.ch/publications/crn_team

Questions and Discussion

“The problems of today will not be solved by the same thinking that produced the problems in the first place.”
Albert Einstein

Contact Information:
Bradford Wilke
Email: bwillke@cert.org
Phone: +1 412 268-5050

Postal Address:
CERT Survivable Enterprise Management Group
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, Pennsylvania 15213-3890
USA