Report on Best Practices for a National Approach to Cybersecurity

Creating National Incident Management Capabilities: Watch, Warning, Response and Recovery

September 17, 2007

Jordana L. Siegel

National Cyber Security Division
Department of Homeland Security

Homeland
Security

National Incident Management Capabilities

- Government imperative:
  - Greater reliance on Information and Communications Technology
  - Greater potential impact from disruption
  - Greater likelihood of disruption – growing threats
  - Need for capabilities at the national level to prepare for, detect, manage, and respond to incidents that occur
  - Effective incident management requires coordination across and collaboration with government, industry, academia, and with the international community
- Primary considerations: Funding, Human Resources, Training, Technological Capability, Stakeholder Relationships, Legal Requirements

Overarching Goals

- Develop a coordinated national cyberspace security response system to *prevent, detect, deter, respond to, and recover from* cyber incidents

- Establish a *National focal point* for managing cyber incidents that brings together government and industry components 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 coordinate effectively in a crisis

Identify or Establish a National Computer Security Incident Response Team (N-CSIRT)

- Need a focal point within government
- Coordinates defense against and response to cyber incidents
- Serves as a single point of contact for cyber security incident reporting, coordination, and communications
- Mission should include analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure

N-CSIRT Functions

- Detecting and identifying anomalous activity
- Analyzing cyber threats and vulnerabilities
- Disseminating early warning information
- Establishing trusted communications mechanisms and facilitating communications among stakeholders to share information and address cyber security issues
- Developing mitigation and response strategies and effecting a coordinated response to the incident
- Tracking and monitoring information to determine trends and long term remediation strategies
- Publicizing general cyber security best practices and guidance for incident response and prevention

Establish Mechanisms for N-CSIRT Coordination with Stakeholders

- Need to disseminate and receive information, including current vulnerability and threat information
  - Government
  - Industry
  - Academia
- Coordination mechanisms can take a number of forms:
  - Maintain a website for exchanging information
  - Provide information via mailing lists, newsletters, trends and analysis reports
  - Produce publications that include alerts, tips, and information about various aspects of cyber security including new technologies, vulnerabilities, threats, and consequences

Ensure N-CSIRT Coordination with Industry

- Establish collaborative relationships with industry to prepare for, detect, respond to, and recover from cyber incidents
- Encourage collaboration to foster sharing of operational information in real time
- Develop and implement programs that ensure the protection of proprietary data
- Define roles and responsibilities for incident management and establish protocols for use over time

Establish Points of Contact with N-CSIRT

- Need to establish points of contact and working relationships with government entities, law enforcement, industry, and international partners for consultation, cooperation, and information exchange
  - Build situational awareness
  - Promote early warning of potential cyber incidents
  - Enable exchange of information about trends, threats, and response activities
- Establish contacts based on departmental functions rather than individuals
- Maintain contacts for accurate dissemination of information and coordination

Participate in International Cooperative and Information Sharing Activities

- Cyber incidents are not be confined to national borders
- Need to build trusted communications with other governments and foreign incident response communities
- N-CSIRT can establish formal and informal mechanisms to facilitate regular information sharing

Develop N-CSIRT Tools and Procedures

- Need for technical tools and coordination plans
  - Standard Operating Procedures (SOPs)
  - Guidelines for internal and external operations
  - Security policies for coordinating with stakeholders
  - Implementation of secure information networks for CSIRT operations
  - Secure communications
- Training for new staff

Develop N-CSIRT Capability to Respond and Recover

- Prepare to address response and recovery efforts from large-scale cyber attack
- Coordination is paramount
- Serves as central point of contact for coordination of operations across the government and with industry
- Need to develop plans and procedures in advance
- Conduct exercises to test plans and procedures

Promote Responsible Disclosure Practices

- Need to protect sensitive vulnerability information
- Manage public disclosure when vulnerabilities in technology products are discovered
- Share vulnerabilities with vendors to facilitate the development of an adequate patch or solution from the vendor prior to potential public disclosure

Questions?

U.S. DEPARTMENT OF HOMELAND SECURITY

Homeland Security