King County

Pacific NorthWest
Economic Region

PSE PUGET SOUND ENERGY

TransCanada
In business to deliver

Microsoft

Infrastructure Interdependencies Tabletop Exercise

BLUE CASCADES II

Held Sept. 8, 2004
in Seattle, WA.

Executive Summary

Executive Summary

More than 200 representatives from private and public sector organizations convened on September 8, 2004 in Seattle, WA to hold an infrastructure interdependencies tabletop exercise to explore how to improve preparedness in the Puget Sound region. BLUE CASCADES II, hosted by the Northwest Partnership for Regional Infrastructure Security, with support from King County and the U.S. Department of Homeland Security, was a follow-on to the successful BLUE CASCADES I held in Welches, Oregon in 2002. The overall goal of BLUE CASCADES II was to raise awareness of interconnections among the region's critical infrastructures and organizations and associated vulnerabilities. While the former exercise focused on physical attacks and disruptions, BLUE CASCADES II centered on cyber events as well to meet stakeholder needs to learn more about cyber threats, disruptions and impacts.

The Scenario was developed by the stakeholders themselves and focused on attacks that disrupted the business practices and operations of infrastructures and organizations, including critical telecommunications and electric power assets. The scenario was designed to explore vulnerabilities and disruptions, and regional capabilities to deal with threats, cascading impacts and incidence response.

BLUE CASCADES II resulted in a large number of findings and recommendations, many suggested by the participants in their evaluations of the proceedings and by a team of independent evaluators. The next step in the process of identifying interdependencies and associated cyber and physical vulnerabilities will bring BLUE CASCADES II participants back together to discuss these results and develop a set of activities and pilot projects (an Action Plan) to improve regional readiness. This Action Plan will be comprised of short-term, low-cost solutions and mid and longer-term actions that will require larger investments. It will build on already existing public and private sector plans and technologies. The stakeholders will work collectively to define requirements, including project leads, oversight procedures, funding needs and sources of support.

Leadership at the municipal, county, and state level will be essential to the successful implementation of the elements of the Action Plan, particularly the encouragement and support of the Department of Homeland Security (DHS) and other relevant federal agencies. In the end, success in lessening interdependency-related preparedness gaps and achieving a disaster resilient region will depend on the willingness of regional stakeholders to take the necessary steps to make this a reality.

Selected Findings and Recommendations

Findings

General Observations

Significant progress has been made in the Puget Sound region by local governments and many larger utilities and businesses in addressing physical vulnerabilities and related preparedness needs, but much remains to be done.

An information sharing and notification system called Northwest Warning, Alert and Response Network (NW-WARN) has been established that links regional stakeholders. This mechanism still needs to be enhanced to fully meet stakeholder requirements.

Understanding Interdependencies and Cyber Threats and Disruptions

Most organizations were aware of interdependencies and their importance and saw the need to focus on developing a comprehensive regional preparedness strategy. They were less knowledgeable about interdependencies that could impact service providers on which they were dependent and the extent/duration of disruption of these services.

Cyber threats, vulnerabilities, and disruption impacts are not well understood by most organizations, which tend to overestimate the technical capabilities of their computer networks to withstand attacks and recover quickly. Few have cyber incident response plans or procedures. For those that do, these plans are rarely tested.

Some organizations have policies to shut off Internet access during a suspected attack. Some resort to manual operations, although they may not be able to sustain such procedures beyond a limited timeframe and may require additional manpower and equipment and transportation to the affected sites—difficult or impossible during a regional disaster and particularly a terrorist event.

The impacts of rolling blackouts and prolonged outages on interdependent infrastructures are not well understood, and organizations want more information on their effects on continuity of operations and business processes.

Integration of traditional emergency management/physical security functions and cyber security remain rare within organizations because of differences in terminology and culture.

Local and State Emergency Operations Centers (EOCs) lack procedures to determine when they should activate for a cyber event. There are no threshold criteria to determine a significant attack is underway and no means to secure necessary information from affected organizations to judge the extent and impacts of a disruption.

There appeared to be minimal cross-organizational communication or interaction to identify and assess interdependencies; coordination across organizational "stovepipes" rarely occurs and smaller public and private sector organizations are not involved.

Cooperation and Coordination

There is increasing involvement by private sector organizations in regional preparedness planning, but the level of this involvement is still quite low. Utilities with a tradition of involvement in mutual assistance agreements showed the most advanced levels of cooperation for emergency response.

Private sector organizations are unclear about the role of the various levels of government in a region-wide disaster. They are reluctant to contact government agencies unless necessary because of concerns that their information could be subject to public disclosure, which could impact their market value.

Organizations do not commonly share information about security issues or disruptions with others, making it difficult to gauge the magnitude of threats, the cause of a disruption, and in case of an attack, the extent of the damage done.

Cross-border issues were not meaningfully addressed in the exercise, e.g., U.S.-Canadian interdependencies and associated challenges in the areas of communication/ information sharing, coordination, and roles and responsibilities.

Communications and Information Sharing

Although many government and larger private sector organizations demonstrated they have redundant forms of communication in place, exercise participants did not seriously discuss the impact on communications if power and telecommunications outages and rolling blackouts continued more than a few days.

It is unclear how Emergency Operation Centers (EOCs) would be activated or communicate with law enforcement or first responders if both cell and wired communication systems were down and the 800 MHz system was also down.

There are no criteria for what constitutes a cyber threat or attack that can provide guidance to stakeholders as to what should be reported. Also, organizations do not know how and to whom they should report a cyber attack, what information to convey, what would constitute a crime scene, or what information should be preserved for evidence.

There is a need to develop ways to share accurate, real-time information to understand interdependencies and how to respond/recover from regional disasters.

At the same time, the private sector is adverse, for proprietary and legal reasons, to share necessary data.

There are impediments associated with sharing classified information with private sector organizations. While security clearances are available to personnel with a “need to know” through the FBI and other federal government agencies, such clearances are difficult to obtain in a timely manner, if at all.

Roles and Responsibilities (Incident Management)

Many participants described cyber incident management as “confused” or “loose.” The federal government has a number of organizations that have missions to respond to cyber incidents and there are also state and private sector response organizations and vendors.

It was not clear to participants what role DHS elements and other federal agencies would play in a regional terrorist attack, physical or particularly in cyber incidents.

Resource Management

Exercise participants generally sought information and resources based on established plans and procedures, but when forced by circumstances to look outside their own organizations, they were unaware of where to turn for assistance. If they did know where resources could be available, they did not know how to access them.

There is no inventory of resources that could be utilized in a regional emergency or a resource management strategy to set priorities and oversee their planned allocation.

It was not apparent in the exercise how local law enforcement and first responders would have the resources to handle the terrorist attacks described in the scenario.

The private sector has resources that could be used in disasters that could be incorporated into regional preparedness planning. Legal and liability issues should be worked out in advance through mutual aid and other agreements.

It is unclear what DOD assets could be available for use in a regional emergency and how such assets would be integrated into response and recovery efforts.

Public Information and Education

The scenario raised a number of questions, including: when should the public be informed, what information is provided and how is this information disseminated and by what organization(s)?

Private and public sector employees, including community institutions, need to have education and training on what they need to do in major emergencies and understand state and local plans and requirements.

There should be a single point-of-contact for disaster preparedness for each stakeholder who is responsible for interfacing with other POCs within regional organizations.

Recommendations

Develop a collaborative initiative to identify and map regional interdependencies and develop the analysis systems that can assess linkages and impacts of disruptions, ascertain preparedness gaps and determine cost-effective mitigation measures.

Develop criteria to enable stakeholders to better determine when a significant cyber attack is underway rather than just a nuisance incident.

Encourage organizations to integrate their emergency management, physical and cyber security and incident response activities and personnel to provide a comprehensive approach to disaster preparedness.

Develop tutorials on impacts of electric power outages, rolling blackouts and power surges on infrastructures, and other types of outages.

Create a regional Cyber Security Council within the Partnership for Regional Infrastructure Security to foster collaboration and to establish cyber emergency response and recovery protocols.

Develop a regional cyber emergency response/recovery plan that includes notification and threshold criteria for standing up EOC's for cyber attacks.

Develop a region-wide "yellow-pages" of points-of-contact for disaster preparedness for regional stakeholders and determine means to keep it up-to-date.

Assist in the development of a model continuity of operations plan for small and medium organizations that focuses on interdependencies and cyber disruptions.

Undertake cyber vulnerability assessments of regional EOCs and other emergency response centers that can help identify cost-effective mitigation strategies to improve survivability and redundancy of IT and communication systems.

Conduct a series of seminars/ workshops to expand general knowledge of cyber threats, attacks, disruptions, impacts and response and recovery.

Hold targeted exercises and workshops to further explore regional interdependencies, including those that go beyond state and national borders. Also use these events to test current practices, including resorting to manual operations, as well as preparedness improvements to address physical and cyber events.

Conduct an interdependencies seminar or exercise to specifically examine U.S- Canadian cross-border disaster response issues and incorporate the lessons learned into bi-lateral discussions on cooperative activities to address vulnerabilities and facilitate response and recovery in regional emergencies.

Develop a dictionary of terms and acronyms that includes cyber terminology to begin building a common language that all stakeholders can understand.

Develop guidelines that take into account legal and proprietary issues to instruct organizations on when, how, and whom to notify about serious cyber problems.

Explore ways to provide expedited federal security clearances to enable dissemination of threat and other classified information to those in key stakeholder organizations who have a "need-to-know."

Further develop NW-WARN as a regional mechanism for alerts/threat warnings, and sharing information, and include cyber issues as a focus. Ensure that cyber security officials of infrastructures and other organizations are included in NW-WARN.

Explore establishing a regional Information Sharing and Analysis Center to enable key stakeholders to better exchange and assess physical and cyber threat-related information in a trusted environment.

Develop a better understanding among stakeholders of the National Response Plan and the National Incident Management System (NIMS) and how regional unified command will operate during a cyber attack. Explore the feasibility of incorporating key private sector organizations into NIMS.

Encourage the federal government to identify a single point of contact within the U.S. Government to respond to cyber emergencies.

Encourage the state to take the lead in working with city, county, federal government, and other relevant organizations in developing a roadmap of their roles and responsibilities and what emergency services they offer.

Leverage existing efforts to develop a regional resource management plan that includes the oversight of prioritization and allocation of equipment, supplies, and mission essential personnel in major emergencies.

Develop a certification program for maintenance, medical, and other critical private sector personnel who will need to provide essential services in a regional emergency to enable them to travel unimpeded through security roadblocks or to cross into other jurisdictions. Provide law enforcement with training as part of this program.

Investigate how military and broader DOD assets could be employed in the event of a regional disaster. Incorporate these assets into regional preparedness planning and test use of these assets in future regional exercises.

Establish a Web-based information resource for regional stakeholders that can be used to provide useful data for stakeholders and to function as a coordination and scheduling mechanism for exercises, seminars, conferences.

Develop a training course for private and public sector employees, including community institutions, on what they need to do in major emergencies and familiarize them with state and local plans and requirements.

Develop a training course for public information officers and media on physical and cyber threats and impacts and include these individuals in workshops and exercises.