Regional Energy Critical Infrastructure Resilience Conference

In association with National Energy Technology Laboratories

Report of

The Conference on Critical Infrastructure Resiliency

October 29-31, 2007
Holiday Inn Select, University Center
Pittsburgh, PA

See *www.CNP.Pitt.edu/CIRconference* for conference agenda, sponsors, participants and press

INTRODUCTION

Observers of military strategy warn that planning for the next conflict may fall short if it is reduced to "fighting the last war." With each commemoration of the 9/11 attacks and Hurricane Katrina, our country is challenged both to learn from the past as well as to avoid "failures of imagination" that the 9/11 Commission observed.

Homeland security entails being prepared for "all hazards." In addition, all response to crisis begins locally. Thus, not only local governments but also locally-based businesses must work to restore social stability and free commerce in the event of disruption – no matter the cause. This restoration is known as "resilience."

At the ***local level***, responders have made numerous strides since 9/ll and Katrina in refining response plans, creating mutual aid agreements, and procuring equipment that enhances resilience in an emergency. At the ***federal level***, guidance and programs from the Department of Homeland Security have encouraged local capacity building for resilience within and across various infrastructure sectors (e.g., energy, banking, communications and healthcare). ***States*** also are players in local resilience planning and have an important role in decisions and resource allocation in our system of government.

In our vast and varied economy, 85% of the critical infrastructure is owned or operated by the private sector. Given this reality, and the operations of large firms across state

boundaries, it appears that collaboration for resilience is emerging at yet another level -- in ***multi-state regions***.

As a result of discussions across states, sectors, and institutions, leaders at the University of Pittsburgh, West Virginia University, and Carnegie Mellon University organized a Critical Infrastructure Resilience Conference held in Pittsburgh in October 2007. Building on the success of a workshop held in July 2006 in Morgantown, WV, the conference provided: 1) a platform for a 'live' exercise in cross-sector communication; 2) a venue for exchanging information, and 3) a forum for discussing potential collaborations across state and sector boundaries.

An executive summary of the conference appears below, followed by summaries of:

- Day 1 live exercise
- Day 2 presentations
- Day 3 'lessons learned' and possible 'next steps'

Appendices to this report include: ***[NOTE these may be considered optional if the web site is still up and covers some if not all of this information]***

- [Summary of conference evaluations] *[Rusty]*
- [Printout of control panel display used in exercise] *[Matt]*
- [Listing of mapping and other internet-accessible resources used in exercise] *[Matt]*
- [Bibliography of references from Department of Homeland Security related to critical infrastructure resiliency ***– aren't these already in 06 Morgantown web site?***] *[Rusty]*

Kindly direct comments or questions about this report to:

Ken Sochats
Director, University of Pittsburgh Center for National Preparedness
Director, University of Pittsburgh Visual Information Systems Center
707 School of Information Sciences (SIS) Building
135 North Bellefield Ave.
Pittsburgh, PA 15260
(412) 624-9416
Sochats@pitt.edu

EXECUTIVE SUMMARY

Organizers: Led by The University of Pittsburgh, West Virginia University, and Carnegie Mellon University, the invitation-only Critical Infrastructure Resiliency (CIR) Conference was held October 29-31, 2007 in Pittsburgh, PA.

Purpose: The Pittsburgh conference had three goals:

1) To understand the interdependence of critical infrastructures that would be stressed during a natural or man-made crisis and ***identify areas for in-house improvement;***

2) To conduct and reflect on a tabletop exercise previously rehearsed by the City of New York to ***rehearse communications capabilities*** across sectors;

3) To offer opportunities to ***consider regional initiatives to promote resiliency***, including a) research and development projects; b) collaboration mechanisms; and c) future conferences and workshops that promote resiliency.

Terms:

Resiliency refers to the capability of a system to maintain its functions in the face of change and to degrade gracefully when it must, whether the change is prompted by a naturally occurring event (such as a hurricane) or a man-made event (such as a terrorist attack or industrial accident).

Critical infrastructure refers to 17 sectors in the National Infrastructure Protection Plan (NIPP): 1) agriculture/food; 2) defense industrial base; 3) energy; 4) public health/healthcare; 5) national monuments; 6) banking/finance; 7) drinking water/treatment systems; 8) chemical facilities; 9) commercial facilities; 10) dams; 11) emergency services; 12) commercial nuclear reactors, materials and waste; 13) information technology; 14) telecommunications; 15) postal/shipping means; 16) transportation; and 17) government facilities.

Participants: Attending the conference were representatives from **[5]** states and more than **[40]** businesses and federal, state, and local agencies. Invitations were extended mainly to senior professionals responsible for restoring critical services or communicating with the public in a crisis.

In addition, WTAE reporter Andrew Stockey (host of Pittsburgh's "Channel 4 Action News This Morning") played the role of "reporter" during the exercise and offered his reflections on role of the media in a crisis. (Stockey covered the conference in an October 30 WTAE report (*see CIR web site*); other conference coverage included an article in the October 22 issue of the University of Pittsburgh *Chronicle.*)

Sponsors: Conference sponsors included the Pennsylvania Office of Homeland Security; the American Red Cross; the University of Pittsburgh Medical Center; the John P. Murtha Institute for Homeland Security; Verizon Business; Ericsson; the Pittsburgh Regional

Business Coalition; Region 13; and the Joint Readiness Center. ***[Ken, please ensure this list is comprehensive.]***

Activities:

DAY 1: The first day of the conference featured a live tabletop exercise led by Verizon Business. Patterned after a similar drill held in New York City after 9/11, the exercise required dividing participants into four sector groups: 1) Energy/Utilities; 2) Healthcare; 3) Government/Education; and 4) Business/Finance. Participants deliberately were given roles outside their expertise to encourage understanding of sector interdependencies.

Participants were placed in loosely defined roles where they had numerous opportunities to communicate across sectors. Decisions came in response to new and compartmentalized information generated by the exercise controller during four exercise segments. All communication appeared on laptop control panels designed for each sector and networked by the Visual Information Systems Center at the University of Pittsburgh.

DAY 2: Participants were offered presentations on existing and new approaches to restoring critical services, mostly from speakers at the federal level. Featured speakers included **James Powers**, Director, Pennsylvania Office of Homeland Security; **Jenny Menna** of the National Cyber Security Division at U.S. Department of Homeland Security (DHS); **Paul Hightower** of the DHS partnerships team; and **Robert W. Reed** and **John McIlvain** of the U.S. Department of Energy Office of Electricity Delivery and Energy Reliability.

A full list of speakers is available on the agenda page of the conference web site; in addition, all speaker comments are summarized in the report that follows.

DAY 3: Participants were given opportunities to share "lessons learned" as well as ideas for regional initiatives and university research priorities. A sampling of ideas from the Day 3 "synthesis and brainstorming" session follows:

- "Internal employee knowledge and roles need to be tested and communicated."
- "How to return people to work should be planned, perhaps on a geographic basis."
- "When and what to communicate with customers should be understood pre-crisis."
- "Communication between businesses should be in the form of pre-planned MOUs."
- "Backup communication is needed; we assume cell phones and web are available."

- "Firms should pass on a knowledge base for new business continuity coordinators."
- "Professional groups, universities, and response groups are good planning resources."
- "Business should understand how local crises escalate up the chain to the Feds."
- "Information 'silos,' and the physical and psychological distance between sectors need to be bridged for effective crisis response."

Next steps: At least three areas were identified where follow-on steps might be useful:

1. ***Providing businesses with an understanding of how and when management of crises by local authorities may be assisted by state and federal resources.***
2. ***Sharing across businesses, government and academia special expertise, best practices, 'success stories,' and tools developed and tested in real-world situations.***
3. ***Inventorying and developing ways to share and coordinate regional capabilities.***

Some noted that an added benefit of working on specific projects is their value in creating or enhancing professional relationships and networks that facilitate collaboration in a crisis.

DAY 1 EXERCISE SUMMARY

Purpose: The exercise was designed to help participants:

1) Understand the interdependence of critical infrastructures that would be stressed during a natural or man-made crisis;

2) Identify areas for in-house improvement; and

3) Rehearse communications capabilities across sectors.

Key questions:

- *How did each group work together?*
- *How did the players communicate within and outside their group?*
- *How did they process and interpret ambiguous information?*
- *What lessons were learned?*

Scenario: The scope of the exercise was limited to the 130 municipalities in Allegheny County. The scenario began on the Sunday before Thanksgiving during a Steelers home

game. Storms were associated with a power outage. A small cluster of students visited the emergency room of a university hospital with flu-like symptoms. Other information "injects" included a sinkhole, traffic congestion, a bridge closing, power disruptions, denial of service problems on the internet, an alarm going off at a firm, possible food poisoning, etc.

No single event was a catastrophe *per se*, but the combined effect of various problems and their timing created disruptions across all sectors, news coverage and speculation, and deployment of emergency services and assets.

Procedure:

Infrastructure sectors: All participants were given a role in the exercise. They were assigned to a hotel breakout room corresponding to one of the following four sectors:

1) Government/Education;
2) Energy/Utilities;
3) Healthcare; and
4) Business/Finance

Communication: Each room was provided with a laptop that projected a control panel on a screen. The control panel provided information common to all sectors (such as news reports) in addition to information specific to each sector. Common information appeared on the right side of the screen. "Injects" for specific sectors appeared on the left side.

Each sector room was given the e-mail address of the other sectors, which could be contacted by clicking on a link on the control panel.

In addition, interactive maps of Allegheny County and other mapping and information tools were accessible directly from the internet via the control panel.

Roles: In a separate "control room," Rick Doten of Verizon Business served as the Exercise Controller. From the "control room" Doten was able to view intra-room communication and send information "injects" to the four different sectors. He also used the control room to meet the reporter and hear updates from the sectors during planned breaks. Feedback was used to adapt and inform subsequent exercise "injects" and create new press reports.

Each sector room hosted a conference participant that was a ***facilitator***, one that was an ***evaluator***, and one that was a ***recorder***.

Facilitators: These individuals helped the group decide on roles, provided procedural prompts (but not solutions), and met with the exercise controller for updates.

Evaluators: These individuals rotated to the different rooms and spend 75 minutes in each, according to a schedule. After the exercise, they shared their observations with the entire assembly.

Recorders: These individuals documented the actions and decisions of the group, and helped to keep time.

In addition,

Media: Andrew Stockey of WTAE-TV in Pittsburgh visited the rooms to gather news, hear press conferences called by the sectors, and generate stories displayed on the control panel.

Within each room, the following roles were represented:

1) GOVERNMENT/EDUCATION: City, County, University representatives

2) ENERGY/UTILITIES: Power, natural gas, water, telecommunications, and regional electric power distribution representatives

3) HEALTHCARE: Representatives of a university hospital and non-university hospital

4) BUSINESS/FINANCE: Representatives of a large bank, a small bank, a manufacturing firm, and a biotechnology company

Schedule: Though the exercise was continuous, facilitators reported to master controller according to the following schedule:

9:30 – 10:45	1st SESSION
10:45 - 11:00	Meet controller in control room
11:00 to 12:15	2d SESSION
12:15 to 12:45	Meet controller in control room; box lunches available
12:45-2:00	3d SESSION
2:00-2:15	Meet controller in control room
2:15-3:30	4th and last SESSION
3:45-5:00	All come together to hear evaluators and discuss exercise

Major exercise observations

When the exercise concluded, participants assembled to hear observations by the media representative, evaluators, and exercise controller. What follows are major observations:

MEDIA REPRESENTATIVE: Andrew Stockey thought exercise participants gave him good information whenever possible, and honest answers when they had limited or no information. He explained that the media need as much information as possible to warn the public if there are safety issues. Thus, the media serve as a conduit for passing information to as many people as possible.

One sector group invited him to a press conference that was a reassuring message from one firm that it had survived the crisis and was back in business.

Stockey expressed hope that the same frank exchanges he witnessed during the exercise would continue during real events. The exercise reminded him of the positive information exchanges that occurred during a previous flood in Pittsburgh. These exchanges allowed information to reach many people, which probably encouraged a faster recovery.

EVALUATORS AND EXERCISE CONTROLLER:

INFORMATION

- *Scale of events*: Many groups were waiting for "the big event." Instead, there were a series of small challenges that together represented a more realistic scenario.

- *Information flow*: Some groups felt uncomfortable with lulls in the action; others noted that quieter periods are typical in a crisis.

- *Handling uncertainty*:

    1. One evaluator noted that some of the "chatter" between injects caused confusion, more so than a lack of information. People want to "connect dots" but may "jump the gun."

    2. A key challenge was how to make decisions based on limited information without making premature decisions that could magnify rather than ameliorate the situation.

    3. People often feel uncomfortable working outside their areas of expertise.

    4. It was hard to know if groups were paying attention to the right things.

- *Prioritization*: Sometimes people lost focus on previous information when new reports came in.

- *The media* often play a dissemination role as well as enhance inter-group communication.

- *Use of the internet* varied between groups. Training may help optimize use of information.

ORGANIZATION

- *Chain of command and jurisdiction*: Questions about these topics arose in every group, e.g., how to access government and emergency response resources, who was responsible at the local, state and federal level.

- *Leadership:*

    1. Some break-out groups (e.g., government) appeared to have more unified command and control; others were more decentralized (e.g., sectors with varying entities within a group).

    2. People seem to be able to quickly set up differing but equally effective leadership patterns. On the other hand, the intensity of a crisis can also create fatigue.

    3. Often one person is asked to perform multiple roles in a crisis.

- *Protocols*

    1. For inter-organization communication are as important as those for communication within a sector. One of the team focused work within specific "silos."

    2. Protocols for communication with the media were developed over the course of time.

DAY 1 KEYNOTE DINNER REMARKS

James F. Powers, Jr.
Director, Commonwealth of Pennsylvania Office of Homeland Security

<u>Prepared remarks</u>

Formal federal government involvement in emergency management dates back to 1951, when the process of declaring disasters was codified in law.

Much later (after 9/11), other laws and guidance were created. The Patriot Act created a special magistrate to hear cases with foreign intelligence information. Legislation from 2002 also created a new cabinet-level agency, the U.S. Department of Homeland Security (DHS). In addition, a series of Homeland Security Presidential Directives (HSPDs) was issued by the executive branch.

DHS implements the HSPDs. HSPD-5 created the National Incident Management System (NIMS). HSPD-7 addresses identification and protection of the critical infrastructure.

The NIMS process established the various Emergency Support Functions (ESFs). These help support the 17 sectors identified in the National Infrastructure Protection Plan (NIPP). The goals are to prevent, prepare for and protect against, respond to, and recover from threats that range from terrorism to natural disasters.

There are 120 Pennsylvania resources or assets identified as "critical" at the federal level. Pennsylvania also has designated 380 sites as "critical" at the state level. At the state level, the state police are charged with the "prevent" mission. Their intelligence function will be implemented in part with a new information 'fusion center' with 24 analysts.

The PA Office of Homeland Security helps with the "prepare and protect" mission – but only indirectly. It is responsible for identifying possible threats, for example, and passing information and funds down to local first responders. This role helps localities perform their legal responsibilities as the entities in charge of response.

PEMA and the Office of Homeland Security must respect the laws and protocols that give cities, townships, and municipalities the authority over response decisions in Pennsylvania. These entities can seek assistance from their counties. Above the county level, the state may be involved, but only at the request of local authorities. A 'rule of thumb:' The entity that imposes taxes for a function is in charge of that function. For the purpose of coordination, there are efforts to simplify the process of requesting assistance via a statewide mutual aid protocol.

As to the 'recovery' mission, FEMA is involved at the request of the state.

Governance traditions in Pennsylvania (and jurisdictional control even by tiny school districts) maximize the independence of local communities. But they also create issues and challenges regarding:

- Command and control: Municipal leaders (not EMS or firefighters) ultimately are accountable; therefore, they must be prepared and capable.

- Authority: The Governor cannot make decisions for municipalities and counties.

- Access: The federal government requires each state to have a 911 emergency call system, yet provides no funds. Municipalities face a situation in which everyone wants 911 emergency services, but few want a communications tower near personal property.

- Coordination: The multiplicity of local governments can make it hard to acquire a "common operating picture" as a crisis evolves. It is difficult to identify and respond to a possible threat if there is spotty or nonexistent reporting by municipalities. Information is known at the state level only to the extent it is reported by municipalities.

In this context, guidance from the federal government needs to be melded with structures, traditions and laws of the state to enable effective municipal responses to crises.

Comments on the exercise

- "Not enough information" and "down time" discussed in the exercise wrap-up are common problems in any crisis.

- Local responders should be part of any business emergency plan. The DHS "buffer zone" initiative recognizes that businesses are in charge of what happens on its property. Local responders are in charge outside the boundaries. Coordinating plans for the "buffer zone" is important to maximize the effectiveness of the response, which can translate into saving more lives and property.

- The question of how to protect "volunteers" is a policy issue that currently is being addressed. We want to encourage appropriate citizen participation in crisis response without subjecting citizens to lawsuits.

DAY 2 PRESENTATION SUMMARIES

Private/Public Collaboration for Regional Coordination for Resilience Planning

Paul Hightower
Deputy Director, Infrastructure Partnerships Division, U.S. Department of Homeland Security, U.S. Department of Homeland Security

SUMMARY: Hightower provided an overview of guiding documents that drive the work of DHS and the partnerships division, and explained how industry and government are working together in various consultative councils.

- The National Strategy for Homeland Security, published in July 2002, states:

  The United States will forge an unprecedented level of cooperation throughout all levels of government with private industry and institutions, and with the American people, to protect our critical infrastructure and key assets from a terrorist attack.

- 17 "infrastructure sectors" are identified in Homeland Security Presidential Directive 7. Examples of infrastructure sectors are energy, agriculture/food, government, healthcare and communications.

  - "Critical infrastructure" is distinguished from "key resources." (Examples of key resources are specific government facilities, dams, key commercial assets, and nuclear power plants.)

- Agencies in the government as assigned to specific sectors. They constitute "government coordinating councils (GCCs)." For example, the Department of Agriculture and Food & Drug Administration helped with a sector-specific plan for agriculture and food.

- "Sector Coordinating Councils" contain industry representatives that interact with GCCs.

- SCCs and GCCs send representatives to "cross-sector coordinating councils."

- A threat and risk management framework guides consultative processes in the coordinating councils.

  - Threat and risk analysis centers are being set up to provide watch and warning information to government agencies and private sector representatives. These tie directly into state-level "fusion centers."

  - In addition, DHS sponsors security clearances to private organizations as appropriate.

Risk Based Security Management – Creating Balanced Operating Environments

Jenny Menna
Acting Deputy Director, Strategic Initiatives
Critical Infrastructure Protection, Cyber Security, National Cyber Security Division
U.S. Department of Homeland Security

SUMMARY: Menna's group at DHS is the designated government IT sector partner. It works with producers and providers of IT, such as Microsoft, Symantec, and Sysco. The group also supports cybersecurity across sectors (e.g., consumers of IT such as banks). Menna summarized the evolving work of DHS in the area of cybersecurity.

Aspects of cybersecurity include 1) outreach & awareness; 2) cyber security technologies, software, and strategies; and 3) control systems.

The National Association of State CIOs is an active IT sector group. It helped the IT sector coordinating council publish a cybersecurity plan in May 2007.

It is important to note that the risk assessment process stresses **critical functions** rather than **critical assets.**

- There are six critical functions subdivided into sub-functions for protection and resiliency planning.

- The IT sector is beginning a comprehensive assessment of vulnerability and risk for these. A big part of this work is gap analysis.

Unique features of the IT sector are: 1) it gets **attacked constantly**; 2) often the **attacker is unknown**. In addition, cybersecurity threats vary across a broad spectrum from organized crime to child hackers to nation-states.

A cross-sector cybersecurity working group composed of 90 members includes ANSI, Infraguard, and academic groups. It is the 'go to' group on cybersecurity initiatives.

- It is working on software assurance, briefings, special projects, and metrics.

- It also works with other sectors, e.g., the chemical sector, water, government facilities, energy. The working group helped these sectors integrate cyber risks into vulnerability assessments.

Other initiatives:

- Control systems: Existing or in development are a forum; a self-assessment tool; and industry-accepted standards. This information is for use within organizations.

- Software assurance: To insure software has built-in security.

- Exercises: Cyber Storm II tests procedures and involves four sectors, five states, 10 countries. (Pennsylvania is a state participant.) The cybersecurity group also works with TOPOFF, Forward Challenge, and other exercises.

- Strengthening the IT security workforce: Carnegie Mellon and The University of Pittsburgh are part of a network of 86 National Centers of Academic Excellence. Other initiatives are a Federal Cyber Service (scholarship); development of an IT security "Essential Body of Knowledge," and a framework for IT security workforce development.

DOE's Roles and Responsibilities as Emergency Support Function 12 – Energy

John McIlvain and Robert Reed
DOE Office of Electricity Delivery and Energy Reliability. (DOE-OE)

SUMMARY: McIlvain and Reed discussed the resources and functions of their office. They typically deploy to an area when Emergency Support Function (ESF-12, energy) is activated. As do other responders, they employ an 'all-hazards' approach in their plans.

ESF-12: DOE-OE has 3 primary functions:

1. **Energy system response coordination, on-site response coordination**. The office sends people out to FEMA or state Emergency Operations Centers (EOCs). They also help coordinate responses from Washington, DC with and through FEMA headquarters.

2. **Information dissemination at national or regional level**. In a big event, numerous companies, states and jurisdictions know their problems only. DOE-EM consolidates and publishes the 'big picture' and offers analytical resources.

> For example, they run web sites to post national situation reports to other agencies and national command authorities, and also to the public. This has been done in hurricane situations, for example.

3. **Emergency authorizations.** As a last resort, DOE can use authorities of the federal government to allocate resources in dire situations.

McIlvain and Reed belong to Region III: PA, WV, MD, DE, VA. They are called out by FEMA. As appropriate, they report to both a Regional Response Coordinating Center (RRCC) and National Response Coordinating Center (NRCC).

When a response is indicated, DOE-OE tries to use a unified reporting system. The key to situational awareness is building trust. They put information from utilities into maps and

work with the Army Corps of Engineers (which is responsible for generators) to provide accurate information that can be trusted.

DOE-EM works along the entire Emergency Response Continuum:

- PRE-EMERGENCY
  Exercises, ESF training, site assessments

- CRISIS/EMERGENCY OPS
  Pre-incident preparation, mobilization, activation, response

- POST EMERGENCY
  Emergency stand-down, lessons learned, restoration

Lessons learned from Katrina:

- When there are many different power companies, a collective common picture is needed for agencies such as HHS, and the Army Corps, so that they know where to turn for information on when power will be restored.

- It would be ideal, when building new infrastructure, to have receptacle for use by the Army Corps, so that it could arrive to a site and immediately plug in a generator.

Assessing the Health Sector with Model-Based Vulnerability Analysis Techniques

Harry Mayer
Field Supervisor, Assistant Secretary for Preparedness and Response, Region Three, U.S. Department of Health and Human Services

SUMMARY: Mayer presented a model for determining investments that offer the best chance of improving the resilience of the healthcare sector. The model, used in systems engineering, entails: 1) describing critical networks; 2) identifying component nodes and their relationships, and then 3) focusing on key network relationships for planning and resource allocation. The approach is being adapted for healthcare but could be adapted for use by other sectors.

Some crises, such as earthquakes, cannot be prevented. Thus planning for resilience is essential. Often simple measures are indicated, such as storing backup generators in places other than basements (where floods could ruin them).

The key is to invest funds where they do the most good. How is this accomplished in health care? The challenges are many, including:

- The vastness and complexity of healthcare: There are more than 13 million health care providers, 6000 hospitals, 70,000 pharmacies, 172,000 laboratories and 2500 pharmaceutical manufacturers.

- Jurisdictional variations (laws, procedures, and priorities differ on a geographic basis).

- The fact that health care is a "white box" versus "black box" system, meaning that it is necessary to understand and observe interactions between components of a system.

Given that health care is a complex network of interdependencies, it may be useful to take a network analysis approach. Model-based vulnerability analysis requires:

1. Identifying critical nodes
2. Understanding links and relationships
3. Focusing on what relationships and nodes are critical

An example is the medical supply chain network: A hospital might be connected to medical an equipment manufacturer, a blood supplier, a pharmaceutical manufacturer and a pharmaceutical distributor.

Strategies for reducing risk using this type of analysis include:

- "***Manual" risk reduction***: Choosing measures based on subjective evaluation

- ***Rank-ordered risk reduction***: Funding the highest vulnerability until all resources are spent and then proceeding to the next vulnerability.

- ***Optimal risk reduction*** (like dealing cards): Spreading funds across risks equally and incrementally spending down to zero.

- ***Apportioned risk reduction***: Assigning a share of available funds commensurate to the risk.

This type of analysis is in its early stages. Potentially it could be done at a local level and fed into the national vulnerability assessment methodology.

Resilience: The Gap Between What We Think and What is Real

Mike Todorovich
West Virginia Department of Military Affairs And Public Safety

SUMMARY: Todorovich gave personal examples of the obstacles to readiness at the state level, both from organizational and a psycho-social perspectives. He encouraged continuation of response planning and collaboration efforts independent of these obstacles.

Organizational inhibitors to reality (in risk assessment and resilience planning):

The "system:"

- …Only wants to hear good news. Shortfalls are unpleasant to raise.
- …Is geared toward "quick fixes." But gap analysis may suggest a longer-term plan and resources are needed.
- … Is inclined to "pick low-hanging fruit." But sometimes there is none.

Psycho-social inhibitors that cause avoidance of appropriate planning include:

- The "gap" floats, in that some resilience issues are problems that are larger than we would like to admit. They are not easily measured, nor are they easily fixed.

- For difficult problems, the tendency is for people to keep studying and talking about them (to understand them better) before they proceed to offer solutions.

- Some issues are difficult to imagine. For example, many people think residents of the Washington, D.C. area would evacuate to West Virginia in the event of a radioactive event. Yet it is difficult to get policy leaders to focus on mass migration issues.

- Coordination is also a problem, given the size of our country and human nature. In West Virginia, a system of regional planners helps address problems more quickly.

Another challenge is to "train as we fight and fight as we train." Exercises and a realistic view of possible threats will help when a crisis hits.

Applying Interdependencies Using the Five "W"s

Mike Burks
Mission Assurance Division, Naval Surface Warfare Center Dahlgren

SUMMARY: Burks discussed the approach used by the Navy to make the defense infrastructure more resilient. Through knowledge management, the Navy supports decision makers with solution-oriented analyses. These can be used in the private sector, given the generic properties of the five "Ws," outlined below.

The five "Ws":

- Who supplies commodity?
- What is the commodity?
- Why is there a need for it?

- Where is it applied?
- When is the commodity needed?

Answering these questions is a way of engaging in mission area analysis and support. This exercise also helps with infrastructure characterization and network mapping. Most networks rely on other networks to perform their functions. To understand the risk of a network disruption, it is necessary to understand the risk incurred by supporting networks.

Identifying interdependencies helps answer the 'So what?' question. Engaging in the 5 Ws also helps verify data and identify vulnerabilities. The ideal would be to integrate research results within and across sectors.

The best resilience strategies use a **network approach**, not an asset-based approach. They incorporate human expertise, tools, data, and processes into a holistic picture. Systems engineering approaches are structured and repeatable, therefore applicable for both defense and commercial endeavors.

As an example of the importance of systems analysis for risk reduction, consider how easy electricity is disrupted. Possible causes:

- A tree branch can bring down a line
- A heat wave can cause rolling blackouts
- Hurricanes and other weather events can be disruptive
- Market manipulation can happen, as when California deliberately instituted blackouts
- Deliberate acts can be planned (usually long-lead time equipment is a target)

Another example: 90% of the petroleum infrastructure was shut down on 29 August 2005 by Katrina; and 135 defense fuel support points were affected by Katrina and Rita.

RECOMMENDATIONS

- Use a phased approach to limit initial complexity
- Build out interdependency rules for use by analysts
- Develop tools to support analysts vs. tools that require analytical support
- Consider network operator intervention when modeling impacts
- Standardize data format and define essential data elements
- Ensure data quality through a scoring process

DAY 3 WRAP-UP SESSION SUMMARY

Summary: On the last day of the conference, participants were divided into their exercise groups from Day 1. They were asked to address the following questions:

1. *What lessons did you take away from the Day 1 exercise?*

2. *What actions would you consider promoting or implementing within your organization as a result of the exercise or conference?*

3. *What are the three most important initiatives you feel could help your organization or sector work toward greater resilience?*

4. *Which initiatives would benefit from regional or cross-sector coordination?*

5. *What research or knowledge base would you propose for improving resilience in your organization or sector?*

6. *What strengths might you or your organization share to help improve resilience within your region or sector?*

The Day 3 discussion revealed at least three areas where follow-on steps might be useful:

1. ***Providing businesses with an understanding of how and when management of crises by local authorities may be assisted by state and federal resources.***

   For example, it might be useful to offer education or seminars on: 1) local- and state-specific business and government response frameworks, laws, structures and plans; 2) specific examples of how plans are activated when a local crisis escalates to state or federal involvement; and 3) business-relevant basics of the National Response Plan [recently re-named the "National Response Framework" or NRF] and the National Incident Management System (NIMS).

2. ***Sharing across businesses, government and academia special expertise, best practices, 'success stories,' and tools developed and tested in real-world situations.***

   For example, the electrical power industry has accumulated expertise in power restoration in the last ten years, and academia and industry have made great strides in cybersecurity. Models, case studies, and prototype tools could be shared to encourage players to adapt existing tools to meet their needs (and avoid duplication of effort).

3. ***Inventorying and providing ways to share and coordinate regional capabilities.***

Universities, professional groups such as contingency planning associations, and locally, the Pittsburgh Regional Business Coalition on Homeland Security, are documenting information about assets for possible use in an emergency. Further development of these initiatives might be pursued, together with ways to make information easily accessible (such as with mapping and retrieval tools).

Group reports: What follows is a summary of the replies each group offered in response to the questions posed.

Business group:

- Internal employee knowledge and roles need to be tested and communicated.
    - Firms should pass on a knowledge base for new business continuity coordinators.
    - How to return people to work should be planned, perhaps on a geographic basis.
- Simulations, conferences are good ways to network in advance of a crisis.
    - Professional groups, universities, and response groups are good resources.
- Communication between businesses should be in the form of pre-planned MOUs.
    - Suppliers and vendors need to be included in planning.
    - Public/private partnerships are needed before a crisis, to know what resources are available and to assure implementation of service agreements in a crisis.
- When and what to communicate with customers should be understood pre-crisis.
    - Backup communication is needed; we assume cell phones and web are available.
- Business should understand how local crises escalate 'up the chain' to the 'Feds.'
- Business needs to know where to find updates from local responders.
- Businesses need to become more involved in work PEMA does, and involved not just with first responders but with other businesses.
- For effective crisis response, information 'silos,' and the physical and psychological distance between sectors need to be bridged.

- The business culture needs to change; this is not regulatory compliance.

Healthcare group

- We have to think of 'the unthinkable.' In the exercise, we looked for 'the big one.' Yet it never came. Major disruptions can result from a series of small crises.
- 'Mission creep' was a problem during the exercise; we were disengaged and chaotic.
    - We need to spend more time planning, and to exercise a plan.
    - At the same time, there is no 'cookie cutter' approach.
- Emphasis on employees and staff is needed.
    - In future exercises, staffing shortages need to be taken into account.
    - Firms do not control their suppliers, who may not have same plan and commitment to resilience. Suppliers need to be included in planning.
    - Staffing scenarios need to include more mutual aid planning.
- A useful tool might be to build a matrix and drop-down list with core interdependencies.
    - A central database with all facilities and staff might be useful. Each utility/firm should make its own list and have it in a database for quick referral when needed.
    - A catalog of resources might be helpful. Or a computer model of some sort to predict impact of events. Take advantage of local academic resources.
- Collaboration matters, not just content-area knowledge.
    - Experts need to be prepared to step into a different role as appropriate. Know your niche as an organization and as a staff member. At the same time be prepared to step out of your 'lane' as needed.
    - Developing relationships is important, especially with the rapid pace of change.
    - Community outreach is necessary to build relationships.

    - Participate more in activities and bring in data sharing. Share intellectual knowledge and best practices, and advertise successes.

- We need to learn how DHS relates to local first responders. What is that connection?

    - There is an information gap between local and federal resources. We don't know how to connect up the chain of command within the state and federal system.

Utility group

Planning and sharing:

- It is important to meet in advance and establish expectations as to what each person or group is responsible for. You don't want to learn your gaps in a crisis.

- We need to share plans: Government makes plans, but does not share them with organizations. All stakeholders need them. Vetting provides a reality check and validates assumptions.

- Create relationships before a crisis. Do not assume normal supply chains will be there.

- Use existing baseline planning documents developed for your region. Develop a plan that includes other interdependencies.

- Use developed plans as guidelines and update them periodically. Start with vulnerability and then proceed to gap analysis.

- Planning for "disasters" only is limiting. Plan also for recovery and reconstitution.

- Develop Continuity of Operations Plans (COOPs) and rehearse with tools you would use in an emergency scenario. One firm used only utility truck radios for a drill because it assumed internet and phones were not available.

Communication

- Communicate proactively. Have your plans reviewed by corporate attorneys to ensure that planned messages will not be used later against your firm.

- Centralize communications as much as possible. Also create backup and redundant communication methods.

Regional cooperation

- Ideas for collaboration include rehearsing emergency fuel distribution if a crisis lasts longer than anticipated; and rehearsing emergency communications.

- Cross-sector regional forums are a good way to share information and dispel myths.

  For example, during the exercise many assumed power would be restored first to hospitals. But as an electrical system is rebuilt, it is rebuilt from specific operating nodes which may or may not serve hospitals.

  Also, restoration of electrical power brings the load back up in small increments to stabilize the frequency as start up commences. If this is not done right, the system can crash again. Generators are tripped when the frequency comes back too fast.

Research

- In determining where to target efforts, it may be useful to develop benchmarks from best practice and learn from those who have succeeded in recovery after a crisis. Research institutions should develop a knowledge base.

- The strengths of the energy sector are: developing backup sources; energy control; and backup communications. Some firms also have energy management simulators to simulate blackouts so they can practice rebuilding electrical systems.

Government group

- Plan (not just for a disaster but the recovery phase), practice, and communicate.

- Learn local information and form relationships before a crisis.

- Use the media appropriately, especially in the aftermath of a message.

- Embrace straightforward solutions, like using battery-operated radios.

- Include all populations in planning to survive a disaster.

- Government needs to know who can be counted on for trusted support.

    - Businesses and government need to communicate.

    - Regional partnerships can smooth out communications, and this helps resilience.

- Each stakeholder has a role to play:
    - Universities can train people and bring people together.
    - Government can be transparent and communicate with the public. One question: How much is the government responsible for the risk analysis pertaining to a private firm or non-government sector?
    - Firms can mobilize resources and provide donations (e.g., providing bottled water to an airport if people are stranded).

CONCLUSION

Organizers would like to thank sponsors and participants for their contributions to the conference. Both financial donations and ideas for collaboration were greatly appreciated.

Please view the CIR web site (URL on the title page of this report) for conference-related documents and updates.