Business Continuity: How to Keep City Departments in Business after a Disaster

Shannon Spence, PE
Red Oak Consulting, an ARCADIS group
Agenda

• Security, Resilience and All Hazards
• The Hazards Cycle and Some Definitions
• Continuity of Operations 101
• A role for Standards
• The IT component
Risk Framework Evolution

• Alfred P. Murrah Building, Oklahoma City (April 95)
  – Street closings around White House
  – New consideration of critical infrastructure vulnerabilities

• September 11, 2001
  – 2002 Bioterrorism Act = VA and ERP required for drinking water systems serving $\geq 3,300$
  – Formation of Department of Homeland Security
  – Multiple Homeland Security Presidential Directives (HSPD’s)

• Hurricane Katrina (August 2005)
  – Paradigm shifts to All-Hazard
  – Confirms limits of guns-gates-guards model
Guns, Guards and Gates

Response, Recovery, Resilience
Key Drivers

Homeland Security Act of 2002

HSPD’s 5, 7 & 9
HSPD-7: The NIPP in Basic Terms

**Protection**
- Deter Threats
- Mitigate Vulnerabilities
- Minimize Consequences

**Implement Actions**
- Cyber security
- Exercises
- Increasing awareness
- Personnel security
- Physical measures
- Plans
- Reducing attractiveness
- Redundancy
- Reliability
- Resiliency
- Sharing information
- Training
Incidents are LOCAL

Courthouse

Statehouse

Incident

Whitehouse
### Potential Threats

<table>
<thead>
<tr>
<th>Natural</th>
<th>Man-Made</th>
<th>Both</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ice Storm</td>
<td>Internet Virus</td>
<td>Fire</td>
</tr>
<tr>
<td>Severe Winds</td>
<td>Cyber Attack</td>
<td>Disease</td>
</tr>
<tr>
<td>Tornado</td>
<td>Agro-terrorism</td>
<td></td>
</tr>
<tr>
<td>Hurricane</td>
<td>Chemical Explosion</td>
<td></td>
</tr>
<tr>
<td>Earthquake</td>
<td>Water Poisoning</td>
<td></td>
</tr>
<tr>
<td>Flood</td>
<td>Radiological</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Bio-Terrorism</td>
<td></td>
</tr>
</tbody>
</table>
Incidents happen
And communities are impacted
And communities are impacted
Hopefully this is not the answer

Our Disaster Recovery Plan Goes Something Like This...

HELP! HELP!

DILBERT
By Scott Adams
Agenda

• Security, Resilience and All Hazards
• The Hazards Cycle and Some Definitions
• Continuity of Operations 101
• A role for Standards
• The IT component
Hazards Cycle

- Mitigation
- Response
- Long Term Recovery

- Incident
- Security
- Preparedness
Definitions

• **Business Continuity Planning (BCP):** The effort to provide procedures to resume or restore **critical business processes** following a disruption.

• **Continuity of Operations Planning (COOP):** The effort to assure that **essential agency functions** across a wide range of potential emergencies continue.

• **Continuity of Government (COG):** Preservation of the **institution of government.** Maintaining leadership, delegation of authority and active command and control.
Agenda

• Security, Resilience and All Hazards
• The Hazards Cycle and Some Definitions
• Continuity of Operations 101
• A role for Standards
• The IT component
Layers of Planning

- Continuity of Operations Planning
  - Business Continuity Planning
  - IT Disaster Recovery Planning
COOP Planning Objectives:

• Ensure the continuous performance of an agency’s essential functions during an emergency.
• Ensure the safety of employees.
• Protect essential equipment, records and other assets.
• Reduce disruptions to operations.
• Minimize damage and losses.
• Achieve an orderly recovery from emergency operations.
• Identify relocation sites and ensure operational and managerial requirements are met before an emergency occurs.
Critical Elements of a viable COOP Plan

- Essential Functions
- Delegations of Authority
- Orders of Succession
- Alternate Facilities
- Interoperable Communications
- Vital Records
- Human Capital Management
- Tests, Training and Exercises
- Devolution and Reconstitution
Essential Functions

• Those functions that enable an organization to provide vital services, exercise civil authority, maintain the safety of the general public and sustain the industrial and economic base.
Delegations of Authority

• Who is authorized to make decisions or act on behalf of the department
Orders of Succession

• Provisions for the assumption of senior agency leadership positions during an emergency when the incumbents are unable or unavailable to execute their duties.
Alternate Facilities

• A location, other than the normal facility, used to conduct critical functions in the event that access to the primary facility is denied or the primary facility is damaged.
Interoperable Communications

• Provide the capability to perform essential functions, in conjunction with other agencies and organizations, until normal operations can resume.
Vital Records

- Records that if damaged or destroyed would disrupt organization operations and information flow, cause considerable inconvenience and require replacement or re-creation at a substantial expense.
Human Capital Management

• The process of acquiring, optimizing and retaining the best talent by implementing processes and systems matched to the organization’s underlying mission.

• Critical in ensuring the flexibility required of key personnel during these times of crisis.
Tests, Training and Exercises

- All staff must be educated on their role in COOP plan execution.
- Exercises that simulate various disruptions and practice COOP plan execution must be conducted.
Devolution and Reconstitution

• The capability to transfer statutory authority for essential functions to other employees and facilities.

• The process to resume normal agency operations from the original or a replacement primary facility.
Phases of COOP Development

- Project Initiation
- Identification of Functional Requirements
- Design and Development
- Implementation
- Training, Testing and Exercises
- Revision and Updating
Agenda

• Security, Resilience and All Hazards
• The Hazards Cycle and Some Definitions
• Continuity of Operations 101
• A role for Standards
• The IT component
Standards: The Water Sector example

- G430-09: Security Practices for Operation and Management
- J100-10 Standard for Risk and Resilience Management of Water & Wastewater Systems
- G440: Emergency Preparedness Practices
Purpose: This standard defines the minimum requirements for a protective security program for a water or wastewater utility that will promote the protection of employee safety, public health, public safety, and public confidence.
Requirements:

- a) Explicit Commitment to Security
- b) Security Culture
- c) Defined Security Roles and Employee Expectations
- d) Up-To-Date Assessment of Risk (Vulnerability)
- e) Resources Dedicated to Security and Security Implementation Priorities
- f) Access Control and Intrusion Detection
- g) Contamination, Detection, Monitoring and Surveillance
- h) Information Protection and Continuity
- i) Design and Construction
- j) Threat Level-Based Protocols
- k) Emergency Response and Recovery Plans and Business Continuity Plan
- l) Internal and External Communications
- m) Partnerships
- n) Verification
Requirements:

a) Explicit Commitment to Security
b) Security Culture
c) Defined Security Roles and Employee Expectations
d) **Up-To-Date Assessment of Risk (Vulnerability)**
e) Resources Dedicated to Security and Security Implementation Priorities
f) Access Control and Intrusion Detection
g) Contamination, Detection, Monitoring and Surveillance
h) Information Protection and Continuity
i) Design and Construction
j) Threat Level-Based Protocols
k) Emergency Response and Recovery Plans and Business Continuity Plan
l) Internal and External Communications
m) Partnerships
n) Verification
Standards: The Water Sector example

• G430-09: Security Practices for Operation and Management
• J100-10 Standard for Risk and Resilience Management of Water & Wastewater Systems
• G440: Emergency Preparedness Practices
Resilience is defined as:

*The ability to withstand and/or rapidly recover from an incident.*
The Resilience Gap

Deficiencies in Preparedness

Source: Villigran 2006
J100-10 Utility Resilience Index (URI)

Operational Resilience

• Reflects utility capacity to cope with incidents that disrupt operations

Financial Resilience

• Reflects utility capacity to cope with incidents that disrupt revenue
Sub-index Indicators

1. Emergency Response Plan
2. National Infrastructure Management Plan Compliance (NIMS, ICS)
3. Mutual aid and assistance agreements
4. Emergency power for critical operations
5. Critical parts and equipment
6. Critical staff resilience
7. Business Continuity Plan
Standards: The Water Sector example

- G430-09: Security Practices for Operation and Management
- J100-10 Standard for Risk and Resilience Management of Water & Wastewater Systems
- G440: Emergency Preparedness Practices

Purpose: To define the minimum requirements for emergency preparedness for a water or wastewater utility, including the development of emergency response plan, exercising and updating.
Water/Wastewater Agency Response Network (WARN)

• WARN Agreement
  – Voluntary
  – No Obligation
  – No cost
  – Liability/Workmans Comp
  – Reimbursement process
  – Element of NIMS
  – All-Hazards

UTILITIES HELPING UTILITIES:
AN ACTION PLAN FOR MUTUAL AID AND ASSISTANCE NETWORKS FOR WATER AND WASTEWATER UTILITIES
By Kevin Monkey, American Water Works Association and Ray Riordan, California Utilities Emergency Association

"An ounce of prevention is worth a pound of cure."
- Benjamin Franklin

American Water Works Association
The Authoritative Resource on Safe Water
September 2011 (48)
Agenda

• Security, Resilience and All Hazards
• The Hazards Cycle and Some Definitions
• Continuity of Operations 101
• A role for Standards
• The IT component
Key Information Technology Trends

**Business Environment**
- Increasing need for real-time business information
- Further consolidation of small systems
- Aging workforce; staff turnover

**Operations**
- Increasing need for faster operational response
- Growing control and monitoring needs
- Increasingly stringent regulations
- Aging infrastructure

**Societal**
- Maintaining public confidence
- Changing infrastructure needs

**Cyber Technology**
- Convergence of information and operations technologies
- Increasing use of electronic & wireless communications
- More use of open non-proprietary systems
- Escalating cyber threats and accidents
Layers of Planning

- Continuity of Operations Planning
- Business Continuity Planning
- IT Disaster Recovery Planning
Disaster Recovery Plan Goals

The disaster recovery process consists of defining rules, processes, and disciplines to ensure that the critical business processes will continue to function if there is a failure of one or more of the information processing or telecommunications resources upon which their operations depends.

http://www.sans.org/reading_room/whitepapers/recovery/disaster-recovery-plan_1164
IT DRP Planning Process

• Develop the planning group and set priorities
• Conduct the Business Impact Analysis (BIA)
• Conduct a Risk Assessment
• Develop Business Continuity and Recovery Strategies
• Develop Business Continuity Plan
• Implement plan
• Conduct awareness, testing, and training of the DRP
• Conduct Plan maintenance and exercises
Business Impact Analysis (BIA)

Defines objectives for the recovery of systems and application that support the business processes:
- Recovery Time: Number of hours/days to resume business process
- Recovery Point: Age of data to be restored

Map business processes to the system(s) that support them
<table>
<thead>
<tr>
<th>Classification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mission Critical</td>
<td>✓Mission Critical to accomplishing the mission of the organization&lt;br&gt;✓Can be performed only by computers&lt;br&gt;✓No alternative manual processing capability exists&lt;br&gt;✓Must be restored within 36 hours</td>
</tr>
<tr>
<td>Critical</td>
<td>✓Critical in accomplishing the work of the organization&lt;br&gt;✓Primarily performed by computers&lt;br&gt;✓Can be performed manually for a limited time period&lt;br&gt;✓Must be restored starting at 36 hours and within 5 days</td>
</tr>
<tr>
<td>Essential</td>
<td>✓Essential in completing the work of the organization&lt;br&gt;✓Performed by computers&lt;br&gt;✓Can be performed manually for an extended time period&lt;br&gt;✓Can be restored as early as 5 days, however it can take longer</td>
</tr>
<tr>
<td>Non-Critical</td>
<td>✓Non-Critical to accomplishing the mission of the organization&lt;br&gt;✓Can be delayed until damaged site is restored and/or a new computer system is purchased&lt;br&gt;✓Can be performed manually</td>
</tr>
</tbody>
</table>
Incidents happen
Hazards Cycle

- Preparedness
- Incident
- Response
- Long Term Recovery
- Mitigation
- Security
- Preparedness

ICMA
Questions/Comments?

Shannon Spence, PE
shannon.spence@arcadis-us.com