Business Continuity: It's Not Just an IT Recovery Plan
Intergovernmental and Enterprise Approaches

A Report for the

Intergovernmental Advisory Board

July 2004

Intergovernmental Advisory Board
American Council for Technology

In cooperation with the
Office of Intergovernmental Solutions
GSA Office of Citizen Services and Communications
U.S. General Services Administration
1800 F Street NW
Washington, DC 20405
www.gsa.gov/intergov

Business Continuity: It's Not Just an IT Recovery Plan
Intergovernmental and Enterprise Approaches for Governments

A Report for the
Intergovernmental Advisory Board

Table of Contents

Executive Summary 3

Introduction 6

Business Continuity Approaches 9

- Enterprise Business Continuity 9
- Intergovernmental Business Continuity 16
- Business Recovery and Resumption for Governments 23

Conclusions 28

For further information, contact James Mackison at james.mackison@gsa.gov

Executive Summary

The Intergovernmental Advisory Board (IAB), an advisory board under the American Council for Technology (ACT) consisting of 4 state, local, and federal Chief Information Officers (CIO), is publishing this report to document the need for a business-centric business continuity approach as opposed to an IT-centric approach. To illustrate this need, the study focuses on enterprise-wide and intergovernmental approaches to business continuity.

The goal of business continuity management is to keep operations running in the event of a disruption to normal business processes. As a program, it includes activities such as planning, risk analysis, providing back-up facilities, succession plans, impact assessments and many others. Recent events have raised the profile of business continuity in the minds of government managers. Incidents such as the Year 2000 (Y2K), September 11, 2001 (9-11), Hurricane Isabel and the Northeastern Blackout of 2003 forced governments to deal with the potential and actual loss of systems, communications infrastructure, facilities, and, tragically, lives.

The objective of this report is to identify and publicize some of the experiences and best practices of government managers in business continuity planning. The report highlights Federal, State, and local government initiatives, research culled from numerous studies and trade publications, and award and best practice programs that recognize business continuity practices. The report also analyzes lessons learned from events such as Y2K, 9-11, and the Northeastern Blackout and Hurricane Isabel.

This report is not intended as a how-to guide that covers the basics of business continuity planning. Rather, it seeks to fill the gaps that the IAB has identified in government business continuity programs. Business Continuity is viewed by some as simply an IT exercise. But for successful planning and execution, the business process owners, i.e. the people that provide the services, need to drive the process. As part of a business-driven approach, there needs to be an understanding of the interrelationship of the government's business processes with those of other governments and the private sector. Also, strategies need to account for the potential loss of critical infrastructure.

As shown by responses to the recent Northeastern Blackout and Hurricane Isabel, governments are applying lessons learned from past events to refine and improve their business continuity planning. The New York City Emergency Response Task Force, in a report to Mayor Bloomberg last fall (http://www.ci.nyc.ny.us/html/om/pdf/em_task_force_final_10_28_03.pdf), noted that many businesses continued to operate and financial markets were able to open in the aftermath of the Northeastern Blackout. It also noted that in the past two years, New York's government agencies and citizens have become better prepared to handle emergencies and business continuity plans are more mature. However, there is still room to improve. A recent U.S. General Accounting Office report, "Continuity of Operations: Improved Planning Needed to Ensure Delivery of Essential Government Services," found

that, in the federal government, "many (continuity of operations) plans did not address…essential functions or interdependencies with other entities." Improving will require governments and organizations to address business continuity as an enterprise, involve intergovernmental and private sector partners, and plan for the worst case scenario, including those that require agencies to continue delivering services without the benefit of the regular facilities, communications infrastructure and information systems.

This report finds that:

Government and business are beginning to take an enterprise approach to business continuity planning.

- ◊ Laws, regulations and industry standards for disaster recovery and business continuity plans have made business continuity a higher priority for governments and businesses.
- ◊ For an enterprise approach to work, it is critical that the information and data needed to respond to a disaster and resume operations be made available throughout the organization.
- ◊ As systems begin to support the entire enterprise, governments need to consider the impacts and risks across the entire organization.

Involving intergovernmental and private sector partners in business continuity, beginning at the planning stage, allows governments to maintain critical interdependencies and share resources and facilities.

- ◊ Collaboration should include private and intergovernmental partners. Governments can play a major role helping businesses continue operations, especially smaller business that may not have the resources to devote to planning, back-ups and alternate facilities.
- ◊ Agencies and businesses should know how to interact and collaborate with first responders. Many local governments have created plans to allow business officials access to emergency zones in the event of a disaster so that they can assess damage at their facilities and begin the recovery process.
- ◊ Collaboration can help jurisdictions share resources and facilities in a time of crisis.
- ◊ Working collaboratively requires well-defined and formalized roles, succession plans, official liaisons, and backups that can perform duties if the primary points of contact are not available.
- ◊ Know interdependencies with other organizations, governments and businesses.
- ◊ Partners should be involved at the planning stage.

In addition to disaster response and emergency services, resuming day-to-day operations and continuity of government, especially for the most critical services, should be a major component of any business continuity plan.

- ◊ Taking proactive measures to avoid or lessen the impact of a disruption is important to maintaining operations. Measures include back-up strategies and detailed risk analysis.

- ◊ Know all dependencies on critical infrastructure. Geographic diversity in back-up facilities and systems can lessen the impact when critical infrastructure in one location goes down.
- ◊ Know which applications are most critical and recover those first. For example, a system that supports a function required by legislation or business agreements to provide continuous service is more critical than others.
- ◊ Focus your recovery and resumption efforts at the end-user level.
- ◊ Test your plan.

Conclusions:

Business Continuity is perceived by many in government as the responsibility of IT offices – event occurs, system goes down, IT shop recovers system, business continues. However, because of the reliance on IT throughout the enterprise, business continuity should really be a concern for everyone in the organization, including senior management. This means that it should be factored into business planning, performance measurement, and all other aspects of the business that rely on information to achieve their missions. This enterprise view of business continuity is critical to protecting systems, understanding risks and vulnerabilities, and reducing the impact of a disruption. To accomplish this entails involving all stakeholders, including other governments, the private sector and even the public. It also requires agencies to consider the worst-case scenario – that they may have to continue to provide critical services and accomplish their mission without access to infrastructure on which they rely. This report highlights many examples of governments doing this.

Introduction

Business Continuity is evolving from an IT priority to a business priority. Recent events, beginning with Y2K and September 11th and continuing through last year's Hurricane Isabel and Northeastern Blackouts, illustrate this evolution, and the work yet to be done.

The IAB noted in its January 2000 report, The Silver Linings of Y2K, that better business continuity planning was a byproduct of Y2K preparations. Government agencies started thinking about how they would recover and continue operations in the event of a major business disruption. The attacks of September 11th demonstrated that disruptions can be unpredictable and catastrophic, and business continuity plans should prepare governments to deal with such scenarios. In addition to the obvious and tragic human loss, September 11th was unprecedented in its impact on governments, businesses and critical infrastructure. Millions of square feet of office space and billions of dollars of telecommunications and technology were affected.

In responses to events like Hurricane Isabel and the Northeastern Blackouts, governments applied the lessons learned from Y2K and September 11th, and learned a few more. In both events, pieces of critical infrastructure were lost for a period of days. As a result of Hurricane Isabel in mid-September 2003, 6 million people were left without power, and the impacted area stretched from North Carolina to New York, with Virginia hit hardest. One estimate put damages in Virginia at $1.6 billion, while suggesting it could go as high as $2 billion (Hardy, Michael "Isabel's costs: $1.6 billion," Richmond Times Dispatch, http://www.timesdispatch.com/servlet/Satellite?pagename=RTD/MGArticle/RTD_BasicArticle&c=MGArticle&cid=1031771850781&path=!). The Northeastern Blackout of August 14, 2003 affected a total of 50 million people over hundreds of miles, from Canada to the Midwest and Northeast United States.

One business continuity success was the performance of financial agencies. Federal Reserve Board Governor Mark W. Olson highlighted the coordination among federal financial agencies during the power outage last year in his testimony to the House's Subcommittee on Oversight and Investigations of the Committee on Financial Services. The Federal Banking Information Infrastructure Committee, which consists of federal and state financial regulators, and representatives form the Homeland Security Council stayed in contact through the disruptions. This sharing of information and coordination of response resulted in no significant operational problems for federal financial agencies (http://www.federalreserve.gov/BoardDocs/Testimony/2003/20031020/). The securities markets response to Hurricane Isabel also offers a glimpse into how it should be done. Overall, the hurricane did not adversely affect markets. According to a statement by the Securities and Exchange Commission, "most of the markets, clearing organizations, and other critical market participants within the areas affected by the August power failure operated remarkably well under these trying conditions." The success was attributed to the decade long business continuity planning efforts overseen by the SEC (Written Statement of the U.S. Securities and Exchange Commission Concerning the Performance

of the Securities Markets During the Northeast Power Outage and Hurricane Isabel, http://www.sec.gov/news/testimony/ts102003sec.htm).

The response to Hurricane Isabel also demonstrated the critical importance of backing up systems and information. Some agencies switched to back-up systems and locations outside the impacted areas. For example, the U.S. Department of Transportation moved to back-up systems outside the Washington area. The U.S. Department of Education dispatched staff to their Atlanta back-up site. Local governments, not having the benefit of regional offices located in different regions of the country, had to work overtime to restore services and resume operations (Dizard III, Wilson and Mosquera, Mary "Government agencies ride out the storm" Government Computer News 09/29/03 http://www.gcn.com/22_29/news/23700-1.html)

In a report to Mayor Bloomberg last fall, The New York City Emergency Response Task Force noted in its report "Enhancing New York City's Emergency Preparedness" that many businesses continued to operate and financial markets were able to open in the aftermath of the Northeastern Blackout. It also noted that in the past two years, New York's government agencies and citizens are better prepared to handle emergencies and business continuity plans were more mature. However, the report still identified areas for improvement and recommended a strengthening of communications among government agencies and with the public, creating a more resilient communications infrastructure that can better withstand utilities failures, and better deployment of public and private resources and personnel to respond and recover from a disruption. (http://www.ci.nyc.ny.us/html/om/pdf/em_task_force_final_10_28_03.pdf)

Impacting an area that spanned eight states, three major cities (New York, Detroit, and Cleveland), and approximately 50 million people, the Northeastern Blackout illustrated some of the work left to be done. The grid failure that led to the blackout was itself a symptom of poor coordination and lack of collaboration intergovernmentally. Such regional disasters require a regionally coordinated response. The blackout also showed that governments do not completely understand how dependent their enterprises are on critical infrastructure.

As shown by the responses to the recent Northeastern Blackout and Hurricane Isabel, governments are applying lessons learned from past events to refine and improve their business continuity planning. However, there is still room to improve. Both events illustrated the inadequacy of business continuity plans in intergovernmental coordination, the need to further entrench business continuity as an enterprise concern, and the lack of understanding of our dependencies on critical infrastructure and the reliance of our continuity plans on critical infrastructure

The continued evolution of business continuity as a business concern supported by IT requires a shift in how we approach it. It is no longer just an issue of the business lines waiting for IT recovery to happen. It requires governments and organizations to address business continuity as an enterprise, considering its impact on overall business performance and obligations. It requires coordination intergovernmentally and with the

private sector to involve all partners and stakeholders. It also requires planning for the worst case scenario, including those that require agencies to continue delivering services without the benefit of the regular facilities, communications infrastructure or information systems.

Business Continuity Approaches

Enterprise Business Continuity

As governments continue to adopt enterprise management approaches, business continuity practices must follow suit**.** Governments are moving away from managing E-Government systems as agency-specific resources. Instead, agencies are beginning to view the systems that support their business in the context of overarching architectures that reflect the entire enterprise. In the federal government, the Office of Management and Budget has developed a Federal Enterprise Architecture that links IT systems to business performance and identifies standards and technologies to be used across the enterprise. To assist state and local governments, the National Association of State CIO's is also doing work in Enterprise Architecture development to help "build a technology adaptive enterprise through implementation of an architecture that is responsive to business processes and the supporting technology" (https://www.nascio.org/hotIssues/EA/). Likewise, governments and businesses are beginning to take an enterprise approach to business continuity planning.

Because of the need for an enterprise-wide perspective in business continuity, governments must view business continuity as a business priority rather than an IT priority. Research shows that governments and businesses are beginning to do just that. A recent survey of professionals involved in business continuity planning by Strohl Systems and Contingency Planning & Management Magazine shows that budgets for business continuity are increasing, as are the number of employees involved in business continuity planning ("BCP budgets in the rise" Continuity Central, June 17, 2003 http://www.continuitycentral.com/news0321.htm). Also, responsibility for business continuity planning is beginning to move to areas other than IT, including finance, security, and operations. Another trend that demonstrates the importance of business continuity is the movement towards business continuity certification ("Disaster Recovery Concerns Fuel Certification Process" Washington Technology http://www.washingtontechnology.com/ad_sup/recovery/3.html). More and more, professionals responsible for business continuity are becoming certified. Organizations such as the Business Continuity Institute, Disaster Recovery Institute International, the University of Richmond's Certified Recovery Program, and New York University's School of Continuing and Professional Studies are among the many that offer certifications of business continuity professionals.

Three factors are contributing to the need for an enterprise approach and the higher profile of business continuity within government. One factor is that organizations, including governments, are being required to have plans in place for business continuity as the result of laws, regulations, industry standards, or business agreements. These legal obligations force organizations to make business continuity a higher priority. A second factor is the increasing reliance of organizations on information sharing and communication to perform functions. In order to work as an enterprise, information needs to be communicated across the enterprise. Business continuity must keep the flow of information intact. A third factor is the development of systems and use of

technologies that support the entire enterprise. Maintaining business continuity becomes much more complex when dealing with large volumes of interconnected data that are housed in multiple locations and accessed via several different devices.

Two examples of enterprise approaches to business continuity are the 2002 and 2003 NASCIO award winners in the Business Continuity and Information Security Category. North Carolina, which won the award in 2002, implemented an enterprise business continuity program through its Office of Information Technology Services. Its priorities are the protection of people, data backup, and provision of alternate locations. Recent events such as Hurricane Floyd, tornadoes and Y2K made Business Continuity a high priority for the state. The ITS program provides:

◊ "Dedicated business recovery team members responsible for the program.
◊ Integration of information security and business continuity to help ensure data confidentiality, integrity and availability.
◊ Employee training, guidelines, policies and procedures.
◊ Data backup records, which are copied and stored at an off-site vaulting facility.
◊ Provision of alternate locations, complete with compatible computers, telephones, and up-to-date contact numbers for employees, contractors, and customers.
◊ Alternate emergency systems that are tested twice a year where ITS conducts "hot site" drills at offsite emergency locations.
◊ A flexible plan that responds to diverse situations where ITS staff may be accommodated at an alternate site or provided mobile data centers locally."

(Business Continuity Best Practices in North Carolina, Katherine White, OIS Newsletter, Issue 13: Homeland Security, http://www.gsa.gov/gsa/cm_attachments/GSA_DOCUMENT/13-NorthCarolina_R2GVI8_0Z5RDZ-i34K-pR.htm) For more information visit the state business continuity page at http://www.its.state.nc.us/Support/Security/SecurityRecovery.asp.

The Secure Michigan Initiative, which won the NASCIO Business Continuity Information Security Award in 2003, provides a model of enterprise information security that involves all stakeholders and customers. Using a five phase process, Michigan assessed the current state of security, the desired state of security, conducted a gap analysis between the two, recommended solutions and developed strategic plan for implementing the solutions. The risk assessment included IT security personnel from 11 different government agencies and was based on existing guidance from NIST, GAO, and ISO 17799. The initiative identified six areas to reduce security risk and protect the continuity of operations:

◊ "Security Roles and Responsibilities
◊ Awareness, Training, and Education
◊ Security Incident Management
◊ Computer Security Risk Management
◊ Disaster Recovery
◊ Certification and Accreditation of Applications and Computer Systems"

(http://www.nascio.org/scoring/files/2003Michigan8.doc)

Laws, Policies and Standards

Laws, regulations and industry standards for disaster recovery, continuity of operations and business continuity plans have made business continuity a higher priority for governments and businesses. In some cases, federal or state laws have required business continuity plans. In others, regulations and policies offer guidance for governments to follow to preserve continuity of operations during a business disruption. Also, many organizations are developing standards for business continuity. All of these efforts contribute to raising the profile of business continuity and framing it as an enterprise issue as opposed to an IT issue.

Many laws, enacted and proposed, impact business continuity. The United Kingdom has made enterprise business continuity a priority. In the UK, they have introduced the Civil Contingencies Bill designed to "deliver a single framework for civil protection in the United Kingdom." The bill defines roles and responsibilities for local responders, establishes better communication between local public safety officials and the national government, and improves the planning process. The bill is currently before Parliament for debate. Information on the bill can be found at http://www.ukresilience.info/ccbill/index.htm. In Healthcare, the U.S. HIPAA Administrative Security Compliance Act requires that health providers have contingency plans in place to respond to emergencies. Among the requirements are backup plans and Emergency Mode Operation Plans (http://www.cms.hhs.gov/hipaa/hipaa2/general/default.asp#contingency_guide). State governments are also passing laws that require continuity of operations. The California Facilities Seismic Safety Act of 1994 requires hospitals to be "earthquake proof" by 2008. This requirement includes the IT infrastructure, networks and systems used in them. According to Gerard Nussbaum, a consultant at Kurt Salmon Associates Inc., the cost for hospital across the state to protect against earthquake related damages could cost $24 billion, with approximately 3 billion of that cost devoted to IT upgrades and new technologies to comply ("Earthquake law pushes hospitals to spend big on IT" Computer World, February 16, 2004 http://www.computerworld.com/managementtopics/management/itspending/story/0,10801,90226,00.html?from=imutopstory).

Governments have also published guidance on business continuity. The highest levels of the U.S. Government are involved in disaster preparation and readiness, major components necessary to continue operations in the event of a disaster. The President's Homeland Security Directive 5 (HSPD-5) calls for the establishment of "a single, comprehensive national incident management system." The Initial Disaster Response Plan from DHS seeks to integrate "the current family of Federal domestic prevention, preparedness, response, and recovery plans into a single all-discipline, all-hazards plan." An initial disaster response plan was released on September 30, 2003 (http://www.dhs.gov/interweb/assetlibrary/Initial_NRP_100903.pdf) and the final version is being developed.

The Federal Emergency Management Agency has developed guidance for governments planning for continuity of operations. The Federal Preparedness Circulars 65,66, and 67

guide agencies through the COOP process. Circular 65 contains guidance for contingency planning in the COOP process (http://www.app1.fema.gov/library/fpc65.doc). Circular 66 advises agencies in their testing of and training for COOP plans (http://www.app1.fema.gov/library/fpc66.pdf). Circular 67 covers the use of alternate facilities in COOP plans (http://www.app1.fema.gov/library/fpc67.pdf). Other relevant federal guidance includes the National Institute of Standards and Technology (NIST) Security Handbook, the Federal Information Systems Controls Audit Manual from the General Accounting Office, and Presidential Decision Directive 63 and Executive Order 13231 (http://www.whitehouse.gov/news/releases/2001/10/20011016-12.html), both of which addresses critical infrastructure protection.

In the financial arena, the Securities and Exchange Commission in its Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System called on critical financial markets to recover operations "within the business day on which the disruption occurs with the overall goal of achieving recovery and resumption within two hours after an event" (http://www.sec.gov/news/studies/34-47638.htm).

In addition to laws and government issued guidance, many standards are being adopted by associations. These standards will affect governments as well as businesses. With its NFPA 1600 "Standard on Disaster/Emergency Management and Business Continuity" the National Fire Protection Association (http://www.nfpa.org/), an international non-profit that develops codes and standards for responding to fire and other hazards, has developed a business continuity standard for public and private sector entities. This standard "provides a standardized basis for disaster/emergency management planning and operations in private and public sectors by providing common program elements, techniques, and processes using a total program approach." The standard was actually been presented to the 9-11 Commission by the American National Standards Institute as a voluntary standard to be promoted by the commission and was included in the commission's final report (http://www.nfpa.org/catalog/product.asp?pid=160000&src=nfpa).

Britain's National Standards Body, the British Standards Institute (BSI) developed a guide to Business Continuity Management (BCM). The Institute's "PAS 56 Guide to business continuity management" describes the activities and outcomes involved in establishing a BCM process and provides recommendations for good practices. It provides a generic BCM framework for incident anticipation and response and describes evaluation techniques and criteria" (http://www.bsi-global.com/Local+Authorities/Standards/Emergency+Planning/pas56.xalter). There are also International Standards Organization (ISO) standards that address business continuity. The ISO 7799 Security standards are international standards and codes of practice that cover information security management, including business continuity practices.

Information sharing and communications across the enterprise

For an enterprise approach to work, it is critical that information and data needed to respond to a disaster and resume operations be made available throughout the organization. To work as an enterprise, information needs to be shared across the enterprise. A major consideration for any business continuity plan is communication throughout the organization in the event of a business disruption. This requires knowing who needs to have what information and how to access it. Knowing the abilities of your current communications system and the employees that have functions that are mission critical is necessary for implementing the plan. Once those are defined, a communications strategy can become more proactive, where alerts could be pushed to a list if pre-defined contacts to prevent a potential threat or disruption.

Companies lose market share for every minute of downtime. While governments do not have market share to lose, they do stand to lose the trust of their citizens, and the safety of their communities they serve. Proactive communication with the public can mitigate the effects of emergencies and disasters, and prepare the community for response. This requires governments to develop technology solutions to communicate critical information even in the event of a business disruption. For example, a government needs to be able to communicate evacuation routes in the event of a disaster and needs to think of ways to communicate this information when the normal communications are down (Levithan, Ben "Missing A Step - The Enterprise Guide to Communications-Enabled Business Continuity" Disaster Recovery Journal, Spring 2003).

Mecklenburg County, North Carolina understands the importance of communication across the enterprise in business continuity. The Mecklenburg County Health Department helped to coordinate a multi-agency response to bio-terrorism concerns in the wake of 9-11. The effort focused on communications between agencies and providing information to medical professionals and facilities in the event of a disaster, allowing doctors and hospitals to continue providing care. The initiative involved the Police, Fire and Public Services and Information Department (http://www.naco.org/Template.cfm?Section=Data_and_Demographics&Template=/cffiles/counties/county.cfm&id=37119).

Another important concern is communicating with all key personnel, whether emergency response, IT or health officials. During recent wildfires in California, the California Disaster Medical Assistance Team (DMATCA-6) used an automated notification system to report out to medical assistance teams to let them know where to report for duty. Notifications were received through several devices, including landlines, cell phones, pagers, and e-mail. This communication enabled the team to respond quickly. Many other emergency response agencies are beginning to deploy this sort of system to coordinate medical staff more quickly. (Mahdavi, Frank "Notification Systems Keep Medical Teams Informed" Disaster Recovery Journal - Winter 2004)

In order to recover and resume operations, business continuity relies on knowing where assets are. Applications such as Geospatial One-stop, which is designed to make geographic information available to all levels of government in disaster response, planning and homeland security, need to consider how to share information if critical

infrastructure is interrupted (Moon, George "Business Continuity and Security Rely on Spatial Information" GEO World, May 2003 http://www.geoplace.com/gw/2003/0305/0305ent.asp). In the effort to make disaster-related information available throughout the enterprise, the U.S. Geological Survey maintains over a century of information on water flows in U.S. Rivers and streams and water cleanliness in its National Water Information System Web, winner of the 2002 Government Information Technology Leadership Award. Many rely on this data to avoid potential disasters and business disruptions. Engineers designing hydroelectric plants and workers involved in outdoors activities can refer to the information to ensure that water levels will not adversely impact their efforts (http://www.govexec.com/features/1102/1102gtlaS1.htm).

The Gujarat, India State Disaster Management Authority along with the UN Development Programme developed the State Disaster Resource Network (SDRN) to enable sharing of disaster management plans, data and information throughout the government via its State Wide Area Network. The system stores, processes and produces query-based reports on resources available, vulnerable elements at risk, emergency contacts, disaster history, and hazard profiles. The information is available to all employees at the local, district and state levels. The reports are also available on portable diskettes should the network be interrupted. (http://203.77.201.16/sdrn/, http://www.challenge.stockholm.se/search_view.asp?IdNr=5178)

In Chester County, PA, locations used in disaster response and management by the Emergency Operation Center were digitized and linked to the County's GIS information and mapping systems. Now critical is available to emergency response. Over 60 layers of geographic information in a relational database are linked to the GIS map and available to emergency responders (http://www.naco.org/Template.cfm?Section=Achievement_Awards&Template=/cffiles/awards/program.cfm&SEARCHID=2003emer15). San Bernardino County, CA created an Emergency Map CD, a GIS system that provides access to comprehensive geographic information on laptops and desktops. The system was developed by the County's Sheriff, Fire, and IT Departments. This enables response officials to access the systems whether in the response center or out in the field (http://www.naco.org/Template.cfm?Section=Achievement_Awards&Template=/cffiles/awards/program.cfm&SEARCHID=2003emer12). Both efforts won 2003 NACO Achievement Awards.

Enterprise Systems

Another reason for an enterprise approach to Business Continuity is the continued implementation of enterprise systems. As business processes and operations begin to support the entire enterprise, governments need to consider their vulnerabilities and risks and how they impact the entire organization. Tools and systems used to manage enterprise-wide present new risks and vulnerabilities that must be taken into account in the business continuity planning process.

One example of this is the implementation of Enterprise Resource Planning systems. ERP refers to computer systems implemented to integrate and manage all critical functions seamlessly. Some of the benefits of such systems include, improved access to data, cross-functional integration, ease of use and increased automation. A solution borne from meeting the compliance needs of Y2K has created an entirely new set of considerations for business continuity planners (Gerber, Cheryl "Beating the ERP Learning Curve" Federal Computer Week, July 6, 1999). Viewed as more of an evolution than an implementation, ERP serves to integrate systems and databases that used to be disparate. While this integration results in streamlined processes for the agencies using them, it also means a reduction in the potential points of failure from many to one, a greater impact if the system is to fail. Of course, this doesn't mean that agencies should not pursue these solutions; the potential returns are too great. But it does mean that business continuity should be considered throughout the planning and implementation of such a system. Because of the complexity and cost of such a system, there is a tendency to view BC considerations as secondary. (Michael Gallagher, "ERP systems and business continuity management" (http://www.continuitycentral.com/feature026.htm).

Intergovernmental Business Continuity

Intergovernmental approaches to business continuity are necessary in the event of disruption, as it is rare that a service disruption affects only one government, as shown by the recent Northeastern Blackouts and Hurricane Isabel. As intergovernmental management becomes more pervasive throughout government, business continuity plans will become increasingly complex. Even seemingly isolated events can have impacts that are far-reaching (e.g. a supplier or subcontractor is hit, affecting your operations). Additionally, IT systems are becoming more interoperable and interdependent upon one another. Emerging technologies and component-based architectures will increase these interdependencies. With systems becoming more complex and integrated, the points of failure are more difficult to diagnose and more centralized. Involving government and private sector partners in business continuity, beginning with the planning process, allows government to maintain critical interdependencies and share resources and facilities.

The Blackout of August 2003 illustrated the importance of intergovernmental coordination to prevent disruptions. A critical piece of infrastructure spanning a huge geographic area encompassing many government jurisdictions failed, causing widespread power outages. Because management of this infrastructure was not coordinated, each jurisdiction was subject to events in areas of the country that they had no control over. The disjointed management of the grid system, which led to the blackout, was itself a symptom of poor interjurisdictional planning and a failure to understand our dependencies on other parts of the country to preserve our operations.

Working with partners requires governments to know their interdependencies with other organizations and groups. Much as there is a supply chain in the private sector, there is a service chain in the public sector. Governments rely on relationships with the private sector to provide most services. They also rely on other levels of government and jurisdictions to deliver the services. Also, information maintained by another jurisdiction or level of government can be used to respond to disasters and mitigate the impact of potential business disruptions. For example, collaboration software can take incident command policies and combine them with real time data from multiple agencies. Understanding these relationships and taking them into account in business continuity planning is key.

Working collaboratively in business continuity requires well defined and formalized roles, succession plans, official liaisons to outside groups, and backup officials that can handle the jobs if points of contact are not available. The New York State Forum for Information Resource Management (NYSFIRM) in its report "Supporting the public's Business Continuity Planning and the NYS Government" recommended that "clear responsibility for who will lead and coordinate continuity planning must be established, both within agencies, and as an overarching support for state and local government" as one the three actions necessary to make a suitable business case and action plan for business continuity planning (http://www.nysfirm.org/documents/pdf/whitepapers/bcp_white_paper.pdf). In its July

2002 report on Critical Infrastructure Protection (CIP), the U.S. General Accounting Office noted the U.S. Government needed to be more coordinated and comprehensive in its approach to protecting information systems. It recommended that efforts to protect critical infrastructure "include all relevant sectors, define the key federal agencies' roles and responsibilities associated with each sector, and define the relationships among the key CIP organizations." GAO wrote that at least 50 federal organizations have CIP responsibilities and that the relationships between these organizations are not consistently established (http://www.gao.gov/new.items/d02474.pdf).

Collaboration can help governments share resources and facilities intergovernmentally and with the private sector in a time of crisis. Some agencies and businesses may not have the budget for full back-up facilities. Governments can play a major role helping businesses, especially smaller business that may not have the resources to devote to planning, back-up systems and alternate facilities. Also, agencies and businesses should know how to interact and collaborate with first responders. Many local governments have created plans that allow business officials to have emergency access to facilities in emergency zones in the event of a disaster.

Intergovernmental Business Continuity Initiatives

One major business continuity-related initiative intergovernmental in scope was the Top Officials 2 (TOPOFF 2) terrorism exercise. The effort was mandated by Congress to test the plans and procedures in place to respond to and recover from a terrorist event. Billed as the largest ever terrorism response exercise in the U.S., participants responded simultaneously to two scenarios: dirty bombs were released in Seattle, and Pneumonic Plague was released in several locations in the Chicago area. Twenty-five governments, including federal, state and local government and the Canadian Government, were involved. The exercise illustrated the need for enhanced intergovernmental coordination and improvement in sharing data and information. For more information, read the summary report from the exercise available online at http://www.dhs.gov/interweb/assetlibrary/T2_Report_Final_Public.doc.

The plan for a National Incident Management System (NIMS) was approved in March of this year by U.S. Homeland Security Secretary Tom Ridge as the "first standardized management plan that creates a unified structure for federal, state, and local lines of government for incident response." Officials from all levels of government and sectors involved in homeland security and disaster response participated in the development of the plan. Key elements of the plan are an Incident Command System (ICS), Preparedness, Communications and Information Management, Joint Information System (JIS), and NIMS Integration Center (http://www.dhs.gov/interweb/assetlibrary/NIMS-90-web.pdf).

The Disaster Management (DM) initiative is another example of bringing together intergovernmental stakeholders. DM was among the initial group of Presidential e-Gov Initiatives identified in the U.S. Electronic Government Strategy. The initiative strongly contributes to the ability of the nation's emergency management response organizations to prepare, respond, mitigate and recover from all types of disasters. These responders operate at multiple levels including federal, state, local, and tribal levels and across

geographic boundaries. A key component of the DM program involves developing interoperability standards that will allow information to be shared seamlessly throughout the emergency management community. The DM program is reaching out to state and local partners to accomplish this. By sharing knowledge and working together through these alliances, the program will be able to provide better service to the nation's emergency management community. The initiative has two main components: DisasterHelp.gov, a portal to disaster-related information and services for citizens, public safety and emergency response agencies, and Disaster Management Interoperability Services (DMIS), which consist of tools that allow emergency management officials to share and access information across jurisdictions and organizational boundaries (http://www.disasterhelp.gov/).

The India Disaster Resource Network is another example of intergovernmental collaboration. The program was developed by the Indian Ministry of Home Affairs, with assistance from the United Nations Development Program (UNDP). Using an online portal, the project has developed an online disaster resource inventory that officials from 600 districts within 35 states can access in times of emergency. The inventory allows for decentralized collection of data and controls access so that only authorized personnel can update information. The system allows jurisdictions to align and share their resources in the event of a disaster (http://www.challenge.stockholm.se/search_view.asp?IdNr=5208).

An excellent example of multiple governments collaborating on disaster response and business continuity issues is the Central American Health and Disaster Information Network. The project is based in Costa Rica and involves 6 organizations: the Pan American Health Organization - Regional Office of the World Health Organization, International Strategy for Disaster Reduction, Costa Rica National Risk Prevention and Emergency Commission, International Federation of Red Cross and Red Crescent Societies, Coordination Center for Natural Disaster Prevention in Central America and the Regional Office of Doctors Without Borders. According to the project, its goals are to compile and disseminate disaster-related information, promote co-operative efforts, and improve risk management throughout the region. The network serves a wide range of users in the Latin America and the Caribbean Region. The project strengthens regional, national and local capacities to establish and maintain disaster information and documentation centers and will contribute to the development of the Regional Disaster Information System (http://www.crid.or.cr and http://www.challenge.stockholm.se/search_view.asp?IdNr=5351).

The OK-First Initiative, a Harvard Innovation in American Government Award winner from 2002, improved state public safety organizations' access to weather information and created a decision support system so that public safety officials can act more quickly to respond to and mitigate the damage resulting from weather-related disasters. The program was funded through a federal assistance program and coordinates federally collected weather data with local government decision support systems. This information sharing and analysis of weather can alert officials to potential disasters. One example highlighted on the project web site notes how "one participant used OK-FIRST to estimate that over 6 inches of rain fell in portions of his county. County officials were

then alerted that a particular bridge might fail. The bridge was closed before it eventually washed away." Imagine the potential impact on the community should the bridge fail. For more information visit the OK-First website (http://okfirst.ocs.ou.edu/). A similar example is the State of Washington's Strategic Forecast System. An alternate for the Council for State Governments Innovations Award, the system identifies potential hazards and disruptions that could impact the state. The program integrates GIS tools, federal emergency management systems, satellite data and the Internet to predict hazards and respond to them proactively.

The State of Florida has had success at fusing interagency information for domestic security. The Florida Department of Law Enforcement established Regional Domestic Security Task Forces throughout Florida that included representatives from law enforcement, public safety, emergency management, health, the private sector and other levels of government. The primary responsibilities of the task forces include detecting and preventing terrorist incidents, collecting and sharing intelligence and information, conducting vulnerability assessments, overseeing training of first responders and other specialized individuals/teams, overseeing and promoting the purchase of certain specialized public safety equipment, developing response and recovery plans and conducting public awareness campaigns. Among Florida's achievements in information sharing for business continuity is the recently created Florida Infrastructure Protection Center (FIPC), which is responsible for anticipating, preventing, reacting to, and recovering from acts of terrorism or natural disasters affecting cyber security. Also important to Florida's domestic security planning and response efforts is the Critical Infrastructure Management System (CMIS). CIMS displays Florida's critical infrastructure in multi-layer map format providing text and image information. This system is available to the Regional Domestic Security Task Forces, the State Emergency Operations Center, all county Emergency Operations Centers, Sheriffs, Health Departments and many other police, fire, and first responder agencies (Lisa Hopkins, Florida's Success at Interagency Information Fusion for Domestic Security, OIS Newsletter Issue 13 – Homeland Security http://www.gsa.gov/gsa/cm_attachments/GSA_DOCUMENT/13-FloridaDomestic_R2GVI8_0Z5RDZ-i34K-pR.htm).

The National Association of Counties has honored several counties as examples of intergovernmental coordination in business continuity and disaster recovery. Story County, Iowa involved multiple jurisdictions, agencies and levels of government in its disaster preparedness program. The program convened all of the above-mentioned stakeholders for a testing exercise that simulated a terrorist attack and tracked and assessed user actions in response (http://www.naco.org/Template.cfm?Section=Achievement_Awards&Template=/cffiles/awards/program.cfm&SEARCHID=2003emer11). Baltimore County Maryland's Office of Emergency Preparedness within the Police Department is responsible for preparedness and response plans, facilities, training and equipment. The office serves as a coordinator between the emergency management services of the police department and the Office of Emergency Management, which coordinates the response of Baltimore County agencies. Through this office, the resources of the police department can be used better and

coordinated with other county agencies in response to a disaster (http://www.naco.org/Template.cfm?Section=Achievement_Awards&Template=/cffiles/awards/program.cfm&SEARCHID=2003crim35). In Virginia, three local governments, the City of Richmond and the Counties of Chesterfield and Henrico, began working toward public safety interoperability across the jurisdictions. The three now share the same public safety communications system, allowing them to coordinate when responding to a disaster and improving the jurisdictions' ability to continue operations (http://www.naco.org/Template.cfm?Section=Achievement_Awards&Template=/cffiles/awards/program.cfm&SEARCHID=2002emer32). In Montgomery County, Maryland, officials conducted a multiagency multi-jurisdictional test exercise to determine the county's ability to respond to a bioterrorist attack. The exercise employed some interesting techniques, including live mock victims, and the use of data from Johns Hopkins, which was incorporated into the Disaster Command System to predict the spread of the biological agents using GIS technology (http://www.naco.org/Template.cfm?Section=Achievement_Awards&Template=/cffiles/awards/program.cfm&SEARCHID=2003emer26).

In California, the Local Government Partnership and the Governor's Office of Emergency Services convened a Business Continuity Working Group in the spring of 2002. The group consists of state and local public safety and emergency services officials along with economic development leaders. The group developed an Internet-based toolkit and online clearinghouse to help state and local officials plan for business continuity. Thus far, the group has drafted best practices for developing continuity of operations plans (http://test-www.opr.ca.gov/communities/partnership/business.shtml).

Government partners should be involved at the earliest possible stage, planning, to preserve business continuity. The Washington DC area offers a great example of regional planning for business continuity. From 9-11 to the subsequent anthrax attacks and sniper shootings, the DC area has encountered a number of incidents that required a regional response. The Metropolitan Washington Council of Governments (MWCOG) created the Regional Emergency Coordination Plan, which is recognized as the first regional plan of this sort. The plan was developed jointly by 17 local governments surrounding DC and covers 15 regional emergency support functions. The plan defines regional incidents as "any situation with the potential to disrupt essential services or mobility, or jeopardize public health and safety on a regional basis," and regional emergencies as a "situation that has disrupted essential services or mobility, or jeopardized public health and safety. This situation has high regional impacts and consequences." The plan helps facilitate coordination and communication in the event of an emergency with important emergency alerts, notifications and updates to all devices (http://www.mwcog.org/security/security/download/plan_summary_911.pdf).

Another example of involving partners in business continuity planning is the State of Nevada Security Committee. The committee brings together state department, divisions, boards and commissions to identify and develop security standards processes and issues. The Committee represents 13 different agencies and has developed security policy and 20 standards to guide state agencies. This planning across the enterprise will help the state

better respond to potential disruptions and security threats. (http://www.nascio.org/scoring/files/2002Nevada8.doc). Pierce County Washington began a review of emergency response and preparedness in response to the events of September 11th. The county's response was to form a Terrorism Early Warning and Response Task Force that has all relevant stakeholders as participants, including public safety, health transportation, military and private sector members. This involvement of multiple agencies and sectors led to a richer planning process that will improve the county's response to disasters. This effort won the NACO Achievement Award in 2002 (http://www.naco.org/Template.cfm?Section=Achievement_Awards&Template=/cffiles/awards/program.cfm&SEARCHID=2002emer34).

Public-Private Partnership in Business Continuity

Government relies on the private sector to perform many functions, and business continuity is no exception. Likewise, businesses need to work with and rely on government assistance to recover their operations in a time of emergency. Collaboration should include public-private partnerships in addition to other governments. Governments can play a major role helping businesses, especially smaller business that may not have the resources to devote to planning, system back-ups or alternate facilities. Also, agencies and businesses should know how to interact and collaborate with first responders.

Many cities have implemented emergency access plans for businesses that allow approved recovery officials to enter disaster zones to conduct the assessments necessary to begin the recovery process and maintain continuity of operations for their enterprises. In St. Louis, officials receive access credentials and must have written continuity plans in place as well as training in fields such as incident command, hazardous materials, and structural assessment (Ballman, Janette "City Implements Emergency Access Plan to Aid Businesses" Disaster Recovery Journal, Spring 2003). The cities of New York and Buffalo partnered with the Business Network of Emergency Resources to implement Corporate Emergency Access Systems (CEAS). The systems were developed with the help of numerous public and private entities (Hamowitz, Mark "Partnership Gives New York Businesses Ground-Breaking Emergency Access Credentials" Disaster Recovery Journal, Summer 2002). Since the blackout, many cities have implemented CEAS to allow credentialed business officials to access restricted areas in a time of disaster. Boston has also recently implemented a CEAS (http://www.continuitycentral.com/news01032.htm).

The government can also play a vital role in helping businesses continue operations, especially small businesses. In Denver, the South Metro Denver Chamber of Commerce implemented the Business Continuation and Communication Center, which provides connectivity and access to local authorities, telecommunications, and in times of disaster. Such centers can be implemented anywhere (Villenueve, Gary "Chamber Of Commerce Helps Businesses Stay In Business" Disaster Recovery Journal, Summer 2002).

Los Angeles established the Business and Industry Council for Emergency Planning and Preparedness (BICEPP). Since 1983, this group has fulfilled its mission "to provide a forum for information exchange to enhance emergency preparedness and contingency planning within the business community." BICEPP recently won the California Earthquake Safety Foundation Award for its work. The group provides public and private sector entities with the opportunity to network and discuss disaster issues. Its board of directors spans government levels and industry sectors (http://www.bicepp.org/).

Involvement of the community in disaster response and business continuity is also acknowledged in the "Issues in Public Policy in Emergency Management for Local Communities" created by the Livingston County, MI Department of Planning and the Michigan Municipal Risk Management Authority. The brochure emphasizes the importance of integrating disaster mitigation and continuity into the community planning process (http://www.naco.org/Template.cfm?Section=Data_and_Demographics&Template=/cffiles/counties/county.cfm&id=26093).

Business Recovery and Resumption for Governments

In addition to disaster response and emergency services, resuming critical day-to-day operations is essential to maintaining business continuity. The telecommunications infrastructure, IT systems, and facilities that governments rely on to deliver services are themselves at risk in disasters. A recent report by the U.S. General Accounting Office found that the federal government was unprepared to deliver essential services in the event of "emergencies--such as terrorist attacks, severe weather, or building-level emergencies." (Continuity of Operations: Improved Planning Needed to Ensure Delivery of Essential Government Services, GAO-04-160, February 27, 2004). Therefore, it is imperative for governments to have a business continuity plan in place that provides workarounds in the event of a loss of facilities, telecommunications, electronic data and systems support. Governments should not only plan to keep systems running, and protect them from attack, but also have viable alternatives in place. The emphasis in business continuity has often been on recovery efforts – restoring systems and communications, backup sites, and storage area networks. However, less attention is paid to performing functions without the benefit of communications, facilities, or systems. To successfully plan and execute, it is critical that business-process owners be involved in business continuity efforts and not just wait for the technical groups to recover systems and infrastructure.

There are some approaches governments can take to enable business resumption. First, proactive efforts of forecasting and community outreach can help organizations predict and mitigate the effect of a disruption, allowing them to resume functions and maintain alternate modes of operation during an incident. Knowing your organization's dependencies on critical infrastructure is necessary to determine potential points of failure, and mitigate the impact of a loss of infrastructure on operations. Resuming services also requires governments to prioritize systems for recovery. Governments should recover and resume functions that are most critical first. Also, recovery and resumption efforts should focus on the end-user

Recently, governments have had to rely on *ad hoc* arrangements to maintain operations. While this type of flexibility is important and no one can foresee every possible disruption, preparation can reduce the impact of a disruption and ease the recovery and business resumption process. On 9-11, the New York Office of Emergency Management's Emergency Operation Center was located in the World Trade Center, leaving the city without a centralized place to manage emergency operations. In the time when citizens needed the services most, the city had to look for a facility to manage emergency response, and deliver emergency assistance and relief. Their move to a site on a ship pier was a huge effort that required coordination with and support from numerous public and private entities (D'Auria, Thomas "Facilitation, Cooperation Guide New York City To A Quick Recovery" Disaster Recovery Journal, Winter 2002).

The response to Hurricane Isabel also demonstrated the critical importance of backing up systems and information. Some agencies switched to back-up systems and locations outside the impacted areas. For example, the Department of Transportation moved to

back-up systems outside the Washington area. The Department of Education dispatched staff to their Atlanta back-up site. Local governments, not having the benefit of regional offices located in different regions of the country had to work overtime to restore services and resume operations (Dizard III, Wilson and Mosquera, Mary "Government agencies ride out the storm" Government Computer News 09/29/03 http://www.gcn.com/22_29/news/23700-1.html).

It is important that an organization's response to a disruption be more than simply a disaster response plan. Many agencies are not prepared to recover and resume their day-to-day service delivery. This is especially important for the most critical government services like water and, public safety, health services, etc. A recent U.S. General Accounting Office report, "Continuity of Operations: Improved Planning Needed to Ensure Delivery of Essential Government Services," noted that many business continuity plans did not address critical functions. Plans should address how to resume those services as quickly as possible, even providing service delivery alternatives if facilities or infrastructure are inaccessible (Koehler, Norm "Getting Beyond Just An Emergency Response Plan In The Public Sector" Disaster Recovery Journal, Winter 2002).

Mitigating the impact through proactive planning

Taking proactive measures to avoid or lessen the impact of a disruption is important to maintaining operations. These include items like back up strategies, detailed risk analysis and planning. The best way to mitigate the damage is to predict and anticipate the event. The United Nations Development Programme has commented on the necessity of preparation and proactive planning to respond to potential disasters. It noted that preparation could save millions from natural disasters in developing countries in its report, "Reducing Disaster Risk: A Challenge for Development" (http://www.undp.org/). The report urges governments to:

- "Develop better understanding of the depth and extent of disaster hazards, vulnerability
- Use the best available data and risk analysis as a basis for policy decisions
- Incorporate disaster risk in regulatory procedures, keeping in mind factors that can increase vulnerability, such as dense urban growth in earthquake-prone areas
- Include disaster risk assessment as an integral part of development planning—particularly in post-disaster reconstruction efforts"

One success is the Consequence Assessment Tool Set (CATS), which is used to forecast and mitigate damage as the result of weather-related disasters. In one system, communications, satellite and weather-forecasting tools are combined with real-time information from vulnerable locations. The tool helps responders predict disasters, estimate damages and respond proactively using computer modeling and monitoring. This tool was based on a system FEMA developed with the Defense Department to respond to nuclear disasters. It uses geographic mapping with computerized impact assessments to determine the potential damage resulting from a disaster. All levels of government have access to CATS. The program has been around for over a decade and actually won the Harvard Innovations in American Government Award in 1996.

In Idaho, the state government is employing an enterprise solution with its "Security information and notification process." Security alerts are disseminated to IT staff in all agencies via several communication devices (e-mail, listservs, web newsletters, etc.). By proactively communicating potential security threats to all state IT staff, the government is better prepared to prevent and respond to them (http://www.nascio.org/scoring/files/2003Idaho8.doc).

Another way to mitigate the impact of a potential disruption is by involving the larger community in preparations and prevention. In the city of Medellín Colombia, which is susceptible to natural disasters, the University EAFIT developed Isla Cocom@ - Prevention, Attention and Recovery of Natural Disasters. This program prepares the community for natural disasters by teaching high school students about their community's dependency on natural resources, the impacts of disasters, and what they can do to help recover from and prevent them. This is done to establish a cultural understanding of the value of natural resources and their impact socially and economically. The program creates a community that is, from a continuity standpoint, more prepared to recover from a disaster. In its nomination for the Global Bangemann Awards, they wrote that while one "does not have any capacity to control the natural phenomena, he will create or develop a series of knowledge that will allow him to act in a successful and effective way by means of programs and plans" (www.infoedu.eafit.edu.co/cocoma/desastres-naturales/index.htm and http://www.challenge.stockholm.se/search_view.asp?IdNr=5587). The Community Emergency Response Team (CERT) in Miami-Dade County is another example of preparation to improve the disaster recovery process and maintain continuity within the community. The county trains citizens in disaster preparedness and response to assist emergency management professionals. This program won the NACO Achievement Award in 2002 (http://www.naco.org/Template.cfm?Section=Achievement_Awards&Template=/cffiles/awards/program.cfm&SEARCHID=2002emer9).

Know all interdependencies on infrastructure

During Hurricane Isabel and the Northeastern Blackouts, pieces of critical infrastructure were lost for a period of days. As a result of Hurricane Isabel in mid-September 2003, 6 million people were left without power, and the impacted area stretched from North Carolina to New York. The Northeastern Blackout of August 14, 2003 affected a total of 50 million people over hundreds of miles, from Canada to the Midwest and Northeast United States. As those events illustrate, it is important in planning for business continuity to know your dependencies on critical infrastructure. Just as the events that cause disruptions can sometimes be out of your control, the impact on critical infrastructure can be out of your control as well. It is important not to plan for business continuity in a vacuum and understand that events may require you to use workarounds. If a plan relies exclusively on your telecommunications to communicate in a time of disaster, then there are few options when day-to-day telecommunications are down. Alternate workarounds need to be addressed in the planning process.

Governments are diversifying their back-ups geographically as a means of protecting themselves against disruptions to infrastructure. For example, on 9-11 many companies had alternate locations situated in lower Manhattan, which didn't help much. Alternate locations other than Manhattan would have been better back-up locations, provided that employees could get to the facilities. One tool being explored by governments to diversify geographically is Teleworking. Teleworking protects the agency from losing all capabilities when operations of the main facility are interrupted. The U.S. Office of Personnel Management has identified teleworking as a means to keeping operations running when offices are inaccessible.

Know which applications are most critical and recover those first.
For example, a system that supports a function required by legislation or business agreements to operate continuously is more critical than another function that, while important to the business, may not have legal obligations. Last year the Federal Information System Management Act reviews showed where agencies are in terms of implementing security. The review revealed significant weaknesses across the board, but particularly in disaster recovery and continuity of operations, and more specifically in how they prioritize systems. The GAO also identified prioritization of critical operations as a major weakness.

September 11th prompted many to reassess their continuity and business resumption plans. Governments need to recover quickly and continue to deliver services, even if their operating environment is significantly altered. Among the counties that reexamined business continuity practices was Dakota County, MN, which won a NACO Achievement Award for its efforts. The focus of the plan was to resume critical government operations as quickly as possible. The plan identified critical operations and services, established a team to implement the plan and compile information needed for response. The goal is to recover critical operations within 72 hours (http://www.naco.org/Template.cfm?Section=Achievement_Awards&Template=/cffiles/awards/program.cfm&SEARCHID=2003emer9).

Focus recovery and resumption efforts on the end-user level
Ultimately, it is the end-user who will be required to resume operations in the event of a disruption. However, many back-up strategies for systems and data are not communicated throughout the organization to the end-user. Centralized computing infrastructure tends to be more emphasized than the end-user environment. With succession planning being paramount and business continuity planning responsibilities diffusing throughout the organization, it is important that all documentation and planning be simple and easy to follow for the end-user. Why back-up information if end-users cannot/will not know how to access it in the event of an emergency? According to a recent survey by the U.S. Office of Personnel Management, federal agencies "need to spend more time ensuring that employees understand contingency plans for terrorist attacks and other catastrophic events" (Barr, Stephen "Emergency Preparedness Survey Finds Agencies Lacking" Washington Post, February 25, 2004; Page B02).

Test your plan

Testing your continuity plan is essential to its ultimate success when an event does occur. As shown earlier, testing should include all partners and stakeholders so that operations can be resumed quickly. The aforementioned TOPOFF2 exercise tested governments' response to a scenario where dirty bombs were released in Seattle while Pneumonic Plague was released in several locations in the Chicago area simultaneously. Twenty-five governments, including federal, state and local government and the Canadian Government, were involved. For more information, read the summary report from the exercise available online at http://www.dhs.gov/interweb/assetlibrary/T2_Report_Final_Public.doc.

Forward Challenge 04 tested the continuity of operation plans of more than 40 federal agencies during an exercise May 12-13, 2004. The test was coordinated by the Department of Homeland Security's Federal Emergency Management Agency. The objectives of Forward Challenge were to:

- ◊ Establish an operation capability at an alternate facility;
- ◊ Implement succession and delegation of authority plans;
- ◊ Demonstrate an interoperable communications capability;
- ◊ Demonstrate a redundant communication capability; and
- ◊ Demonstrate the ability to access vital records necessary to conduct normal operations from a designated alternative location.

The test scenario was "all federal government-occupied buildings simulate closure as a result of the combination of events and credible threats of actions from various terrorist groups and individuals." For more information, visit the DHS web site (http://www.dhs.gov/dhspublic/display?content=3554).

In Montgomery County, Maryland, officials conducted a multiagency multi-jurisdictional test exercise to determine the county's ability to respond to a bioterrorist attack. The exercise employed some interesting techniques in the exercise, including live mock victims and the use of data from John's Hopkins, which was incorporated into the Disaster Command system to predict the spread of the biological agents using GIS technology (http://www.naco.org/Template.cfm?Section=Achievement_Awards&Template=/cffiles/awards/program.cfm&SEARCHID=2003emer26).

NASDAQ conducted two disaster recovery tests in early 2004 to determine the effectiveness of its backup facilities, alternate locations and operations through the backup facility in Maryland. NASDAQ companies participated in the test. According to NASDAQ CIO, Steve Randich, the tests showed no weakness and the market served more than 50 of its member companies during the test interruption. Both NASDAQ and the companies' plans were tested ("Nasdaq's Tests Showed No Weaknesses, CIO Says," Computer World, 05/10/04 http://www.computerworld.com/securitytopics/security/recovery/story/0,10801,92987,00.html?f=x56).

Continuity of Government

On September 11th, succession plans proved to be a weakness for some organizations. In some instances, entire senior leaders were tragically lost and the dependency on those key personnel was too great. In addition to continuing to provide services, governments have the added responsibility of continuing governance itself. September 11th showed that attacks could potentially paralyze a government. The harsh reality that an entire legislative bodies, county commissions, or government administrations can be paralyzed by a disaster must be considered by business continuity planners. Continuity of Government plans are necessary to ensure that government is maintained. These plans include lines of succession, delegations of authority in the event of an emergency, alternate locations for government bodies, and processes to reconstitute a government body if a large number of members and leaders are incapacitated. An excellent resource is the National Governor's Association Issue Brief entitled "Planning for Government Continuity" (http://www.nga.org/cda/files/1103CONTINUITY.pdf). Also, the Brookings Institution and the American Enterprise Institute established a commission to recommend how to continue government should an event incapacitate a large number of high-ranking government officials and elected representatives. Its work can be found at http://www.continuityofgovernment.org/.

Conclusions

Business Continuity is perceived by many in government as the responsibility of IT offices – event occurs, system goes down, IT shop recovers system, business continues. However, because of the reliance on IT throughout the enterprise, business continuity should really be a concern for everyone in the organization, including senior management. This means that it should be factored into business planning, performance measurement, and all other aspects of the business that rely on information to achieve their missions. This enterprise view of business continuity is critical to protecting systems, understanding risks and vulnerabilities and reducing the impact of a disruption. To accomplish this entails involving all stakeholders in business continuity, including other governments, the private sector and even the public. It also requires agencies to consider the worst-case scenario – that they will have to continue to provide critical services and accomplish their mission without access to infrastructure on which they rely. This report has highlighted many examples of governments doing this.