DIGITAL GOVERNMENT INNOVATION

Number 2004/01 February 2004

ENSURING SERVICES AVAILABILITY: SEVEN STEPS TO CONTINUITY OF GOVERNMENT OPERATIONS

■ Thomas Foss

A category 2 hurricane carves a new channel in the Outer Banks, isolating a village and cutting off water, sewer, and power services for months. How will you provide these services to the residents who remain on the island?

A severe ice storm takes down trees and power lines, blocking EMS, fire department, and police access to large areas of a Piedmont community. Only through a cooperative effort by the power companies and local governments over several days can the community's services be restored. How will you protect the public safety until the streets are clear and power is back on?

In a bioterror attack, anthrax powder is spread through the county courthouse, and it may take up to a year to remove the contamination. How can the public access property records until the building reopens?

As recent events and preparation exercises have demonstrated, government operations can be disrupted by a variety of events, both man made and natural. Whether the disruption results from a hurricane or from a blackout caused by an ice storm, citizens still expect local government services to be available when they are needed.

Thomas C. Foss is Senior Technical Services Advisor for the Center for Public Technology. His e-mail address is: foss@iogmail.iog.unc.edu.

School of Government
University of North Carolina at Chapel Hill
Institute of Government
Master of Public Administration Program

The Public Health Security and Bioterrorism Preparedness and Response Act of 2002 requires more than 235 North Carolina jurisdictions providing water utility services to conduct security reviews. These reviews can serve as a useful framework for conducting comprehensive reviews of all local services.

In the last few years, information technology (IT) has become a central element in the delivery of many local government services. This bulletin presents a seven-step planning approach focused on IT continuity, but such an approach can be applied to many other government functions as well. Because not all jurisdictions can afford to immediately secure all resources, this approach identifies key processes and their supporting systems as they apply to the unique circumstances of North Carolina cities and counties and expands its focus from that perspective. The emphasis is on service delivery, not specifically on the IT systems which supports these services.

Planning Objectives

Ideally, a disaster plan will never have to be used—the planning process should provide for the implementation of several countermeasures that can prevent many disaster-related disruptions from occurring. If a disaster does occur, however, a good continuity plan will:

- contain the impact of the disaster,
- provide a framework for an organized disaster response,
- minimize operational disruptions, and
- identify alternate ways to support operations.

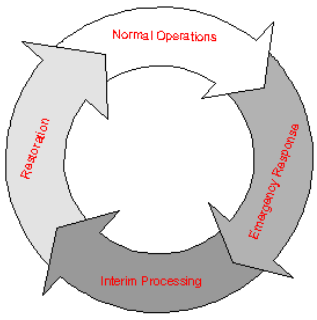

Figure 1: Disaster Life Cycle

Disaster Life Cycle

The objective of continuity planning is to allow a jurisdiction to transition through the disaster life cycle (see Figure 1), moving from normal operations, past the emergency response, and on through interim processing to a restoration of normal operations. Effective planning that allows a jurisdiction to avoid or prevent a disaster is clearly preferable to having to go through the recovery process.

The Planning Process

The Business Continuity Planning Process used by the Center for Public Technology is a seven-step model which looks across the organization to determine where priorities should be assigned—first, to protect against a disaster; second, to minimize the impact of a disaster; and third, to get services up and running as rapidly as possible.

Step 1: Identify Business Processes, Categorizing Criticality

Not every function performed by a government organization is mission critical in the short term. In case of a disaster, whether man made or natural, certain key functions and services—such as 911 dispatch, police/fire/EMS response, utility services, and emergency management operations—must continue to be delivered.

The Center for Public Technology places services into three categories:

- Category 1: mission critical—services that must remain operational at all times
- Category 2: immediate post-incident—services that must be brought back online as soon as possible after an incident
- Category 3: normal services—services that need not be restored in full until the incident has passed and category 1 and 2 services are operational

Step 2: Identify the Assets/Systems That Support Business Processes

When you evaluate your IT infrastructure, you should have a clear understanding of just what computer systems are supporting your operations. During Y2K preparations many local governments conducted extensive IT system inventories with an eye to

assessing the level of dependence on those systems. If available, those preparations should be reviewed for applicability to current operations. If you are starting an IT assessment from scratch, indicate on a list of processes which assets and/or systems support each process. For example, systems that support a category 1 process or multiple category 2 processes should be tagged as mission critical.

Step 3: Conduct Risk Assessments on Each Mission-Critical Asset/System

A *risk assessment* is the systematic review of vulnerabilities and threats to a system and the analysis of the potential impact the loss of information or failure of the system would have on the organization's mission. *Vulnerabilities* are weaknesses in the system, the system's environment, security, internal controls, or implementation that might be exploited to harm the system. *Threats* are circumstances or events with the potential to harm your assets. For example, if you have a system located in a vulnerable place, such as in the basement of a waterfront building, high water is a logical threat to consider.

As you conduct your risk assessment, start by examining vulnerabilities, then consider threats. Vulnerabilities may occur when proper maintenance is not performed or when poor physical planning places assets in locations where they may be easily harmed. Many of the IT system problems that affected government and business organizations in the summer and fall of 2003 resulted from the failure to maintain software at the most current version or patch level. Additional responsibility lies with the programmers who developed the software under attack and thus created the vulnerabilities that were subsequently exploited. Because modern software with its millions of lines of code is increasingly complex, it may never be completely secure. As a consequence, system administrators must be diligent about system maintenance, continuously monitoring vendor update sites and ensuring that all systems in the organization have up-to-date virus protection.

Threats take advantage of vulnerabilities to harm operations. If you are operating a system without up-to-date virus protection, many kinds of malevolent programs, often hidden in e-mail attachments, are a threat to your assets. If your town hall is located in a flood plain and you haven't made provisions to build a waterproof barrier around it, high water is a threat to your assets. The Town of Princeville's infrastructure, for example, was seriously damaged in 1999 by the floods caused by Hurricane Floyd.

Figure 2: Princeville Town Hall, showing the water level of the flood from Hurricane Floyd, 1999

Clearly, for any organization, there are many combinations of vulnerabilities and threats. For that reason plan to have "outside eyes" review your organizational structure and processes—familiarity with your own operations may foster nearsightedness. Bringing in an outside consultant to review your current circumstances can help identify weaknesses and introduce your staff to best practices with which they may not be familiar.

Step 4: Create a Threat Matrix

A threat matrix is an organized array of assets and their associated vulnerabilities and threats. Each asset many have many vulnerabilities, and each vulnerability may make you subject to more than one threat.

Asset	Vulnerability	Threat
Town Hall	Located in Flood Plain	High Water
	No Alarms	Fire
		Burglary
Finance Computer System	Server Located in Unlocked Closet	Tampering
		Theft

Figure 3: Example Threat Matrix

Using the matrix format allows you to carefully review all of your assets and to adjust any elements as necessary to ensure that you have covered all contingencies.

Step 5: Adjust Priority Based on Risk Level

For each combination of asset/vulnerability/threat, assign a risk level, or likelihood, of that specific threat impacting that asset. This step should be performed at regular intervals and your matrix updated based on environmental variables, such as hurricane forecasts or terrorism threat levels. While considering risk levels, remain cognizant of the processes that each asset supports—the most critical processes must have higher priorities assigned to ensure their continuous operation.

Step 6: Identify Countermeasures

Beginning with the most critical processes, examine the threats according to descending risk level, identifying specific countermeasures that can be implemented to mitigate the risk. Often, one countermeasure will serve to remove or reduce the impact of several threats. For example, implementing a firewall to protect your computer network from intrusions can also prevent other types of network attacks, such as denials of service or backdoor penetrations.

Also remember that some assets may support more than one process. You must address the protection of assets that support both critical and multiple processes. For example, an emergency generator required to supply power to your emergency operations center can also, if properly sized and located, provide extended backup power to your computer systems. The Town of Nags Head identifies "rally points," usually inland cities or towns, where town staff move equipment in advance of potential storm evacuations. This location varies depending on the anticipated storm track. During Hurricane Isabel in 2003, the rally point was Rocky Mount. The exact location is determined "at the last possible minute, which may translate to a week before the expected landfall," according to Town of Nags Head Management Information Systems Director Jim Northrup. The City of Kinston has been nationally recognized for its efforts to mitigate the effects of new disasters by developing strategies to purchase property in flood zones and relocate citizens and facilities to higher ground A case study by the Federal Emergency Management Agency (http://www.fema.gov/pdf/fima/kinston_cs.pdf) discusses the efforts the City of Kinston and Lenoir County made to use innovative floodplain management to reduce the damage of future storms.

Step 7: Identify Alternative Processing Solutions

Although implementing countermeasures should markedly increase the resilience of your jurisdiction to respond to disasters, you should be prepared to move your operations to an interim facility—if your city hall or county courthouse is damaged or contaminated, how will you deliver services? Emergency assistance with preservation of records may be available from the North Carolina Department of Cultural Resources. Commercial vendors are available to provide backup locations in other geographic areas, including equipment identical to what you may be operating. The cost of these "hot site" services is substantial, and you may want to consider partnering with other jurisdictions in the state having similar operations and creating a mutual aid agreement. If your IT systems are server based, you may be able to store an emergency server and backup tapes at another less vulnerable location where you can also set up temporary operations.

Preparing Your Plan

Your business continuity plan should clearly identify which services your jurisdiction considers essential, ranking them to minimize conflicts during an emergency. Recovery time objectives (for example, one hour after disaster, one day, one week, and so on) should be established for each service and process, identifying the impact of continued delay in service restoration.

For each service, your plan should specify procedures to be used in the event of a disaster. Because responses differ depending on the type of disaster that has occurred, there are likely to be many different procedures in the plan, some of which are appropriate for a power outage and others, for a chemical spill.

Plan Contents

A good business continuity plan includes:

- identification of the process/service
- the resources required to deliver the service
- the team members responsible for the delivery of the service
- the roles/responsibilities of each team member
- staff lists with contact information, including landline and cell phones, e-mail and physical addresses

- vendor lists and contacts
- inventories of emergency/backup supplies and their locations
- computer hardware and software configuration details, network diagrams, and restoration tapes/CDs
- succession lists, identifying who can fill each role if the primary participant is incapacitated or dead
- supply lists
- prepackaged communications to citizens, including evacuation announcements, disaster declarations, and/or instructions about sheltering and mitigation

Each specific incident procedure should include:

- damage assessment instructions
- damage mitigation instructions
- alternate operating procedures
- temporary location move/setup instructions
- instructions on how to order/recover equipment
- where to get installation help
- how to install replacement equipment
- operating procedures for alternate/temporary locations
- considerations for relocation back to permanent facility

Exercising the Plan

An untested plan may not work as intended. It is important that plans be tested on a regular basis, both to ensure that participants are familiar with their responsibilities and to accurately assess the plan's technical aspects.

Testing should be conducted using a variety of scenarios:

- What happens if your backup location is unavailable or the roads leading to it are blocked?
- Will your equipment fit into the temporary space?
- Is there adequate power at an alternate location?
- Do you have the correct plugs and cables?
- What if your key personnel are not available?

Conclusion

Disasters happen. County, city, and town governments are closest to citizens, providing the first and most direct response in times of crisis. It is imperative that cities and counties make adequate plans enabling them to continue service delivery or, if necessary, to recover those services as rapidly as possible after a disaster. A comprehensive, jurisdiction-wide disaster recovery/ business continuity plan is essential to this process.

Water Utility Disaster Plans

Information concerning the Public Health Security and Bioterrorism Preparedness and Response Act of 2002, including sample water utility disaster plan formats, can be found at www.epa.gov/safewater/security.

Every community water system that serves a population greater than 3,300 is required to:

1. conduct a vulnerability assessment. The basic elements of a vulnerability assessment are described in the Vulnerability Assessment Fact Sheet;
2. certify and submit a copy of the assessment to the Environmental Protection Agency (EPA) Administrator;
3. prepare or revise an emergency response plan that incorporates the results of the vulnerability assessment; and
4. certify to the EPA Administrator, within six months of completing the vulnerability assessment, that the system has completed or updated its emergency response plan.[1]

---

1 . "Community Drinking Water Systems—Requirements under the Public Health Security and Bioterrorism Preparedness and Response Act of 2002," U.S. Environmental Protection Agency, http://www.epa.gov/safewater/security/community.html (accessed October 17, 2003).

(*Disaster Plans continued*)

(*continued from page 5*)

Systems serving more than 50,000 people (of which there are fourteen in North Carolina) were required to submit their assessments in 2003; those serving from 3,300 to 49,999 people (of which there are eight in North Carolina) have until June 30, 2004, to complete their vulnerability assessments. Emergency response plans are due six months after the assessments are sent to the EPA: December 31, 2004, for the smallest jurisdictions; and June 30, 2004, for jurisdictions with populations of between 50,000 and 100,000.

Guidance for the development of the EPA-required Emergency Response Plan can be found at www.asdwa.org.

Web Resources on Business Continuity

1. News sites: All are free; some require registration to access information.
   - www.drj.com
   - www.contingencyplanning.com
   - www.globalcontinuity.com
   - www.disaster-resource.com
2. Continuity vendors: These representative vendors provide support for hot sites, off-site storage of data and records, and mobile disaster recovery. No endorsement of any vendor is implied by its listing here.
   - www.recovery.sungard.com
   - www.ironmountain.com
   - www.agilityrecovery.com/
3. Government sites:
   - www.dem.dcc.state.nc.us—State of N.C. Division of Emergency Management
   - www.hpo.dcr.state.nc.us/disaster.htm—State of N.C. Historic Preservation Office, Department of Cultural Resources
   - www.fema.gov—Federal Emergency Management Agency, now a part of the Department of Homeland Security
   - www.disasterhelp.gov—Central portal for all disaster-related information from the Federal government

Definitions

antivirus. Software that detects and removes harmful software. To be effective, antivirus programs should be updated and systems completely scanned each day. The ability to scan incoming e-mail attachments and files ("real-time protection") is essential.

asset. Any resource that serves a jurisdiction. An asset can be tangible—as in a building, vehicle, computer, or person—or it can be intangible, such as the knowledge of an experienced employee.

backdoor penetration. Also known as a "Trojan Horse," software that is hidden on a system to allow intruders to take control of the system remotely without the operator's knowledge.

denial of service attack. An attack that uses other infected computers to flood a server with data, effectively blocking legitimate access.

(*Definitions continued*)

(*continued from page 6*)

firewall. Software or hardware that prevents access to certain ports on a network. Ports may be blocked completely or may remain open to only certain types of traffic.

key logger. Hidden software installed on a computer that captures every keystroke, tapping into passwords, account numbers, and other private data. Keystroke loggers usually then send the logged data to the attacker's computer via e-mail, allowing the attacker to remotely obtain access to a system.

patch level. Product updates or patches periodically released by software vendors. In some cases these patches offer enhanced functionality; in many cases they correct problems. Keeping all software, including applications and operating systems, at the most current level is essential to protecting a computer or network system.

port. Virtual "ports" on computers connected to a network that uses the common TCP/IP network protocol. Ports are numbered from 1 to 65535 and serve as connection points for other computers on the network. Port 80 is the most common and is used for Internet browsing/World Wide Web access. Unused ports should be closed/blocked at the firewall to reduce the possibility of unwanted access.

threat. Circumstances or events with the potential to harm assets.

virus. Malicious software that spreads through e-mail attachments or Web site programming and can harm your system. Viruses take many forms and can have many different kinds of effects, including erasing data, hijacking e-mail systems to send thousands of spurious messages, or opening a back door for server takeover.

vulnerability. Weaknesses in the system, the system's environment, security, internal controls, or implementation that might be exploited to harm the system.

worm. Specific type of program that may include virus code, which replicates by spreading copies of itself throughout the network. Worms cause major damage by consuming so many resources on the system that the system can only be restored by shutting it down

The Center for Public Technology, UNC Chapel Hill School of Government

The Center for Public Technology responds to the needs of local and state government in order to improve public services and strengthen local communities through the skillful use of information technology.

Objectives include:

- Providing education and training for local government leaders, public managers, and staff professionals in the strategic use of technology and its application to the business of government.
- Facilitating assistance to local governments in technology-related matters.
- Fostering an environment that uses technology to support innovation, change, and leadership.
- Working on applied research projects that help local and state governments develop strong local economies and make the best use of information technology resources.
- Supporting close working partnerships among state and local units of government and the North Carolina University system.

(*The Center continued*)

(continued from page 7)

Technical Assistance Program

The Technical Assistance Program (TAP) of the Institute's Center for Public Technology provides support to North Carolina local governments as they develop and implement security and disaster recovery plans. In partnership with federal government agencies, TAP staff has developed a Security and Business Continuity Planning model that uses best practices developed for defense agencies to guide local governments as they create their own data protection strategies.

Working with NCLGISA, the N.C. Local Government Information Systems Association, TAP staff has assembled a Security Best Practices Team to (1) identify areas in which local governments' IT systems are vulnerable to intruders, (2) develop instruments to assess the degree of vulnerability, and (3) create tools and training that cities and counties can use in protecting their networks and servers from intruders. The team then will assist jurisdictions that need help making their systems more secure.

In addition, TAP provides local governments with technical assistance in the development of jurisdiction-wide strategic information technology plans designed to link IT planning to the jurisdiction's budget development process and to break down the "silos" that separate data in IT systems.