Continuity with Collaboration

The Network Model for Successful Business Continuity Practice

March 2004

OpWatch™ (A Division of Paradigm Solutions Corporation)
Corporate Headquarters
2600 Tower Oaks Blvd.5th Floor, Rockville, Maryland 20852
Phone 800.679.2856, Fax 301.468.1201, Sales@OpWatch.net

Continuity with Collaboration

The Network Model for Successful Business Continuity Practice

> *Corporate executives have a legal duty and a moral obligation to their stakeholders to assure business survivability, but since September 11 it appears as if they are in a state of decision/action paralysis or denial about the need to take action.* (Sikich, 2003)

INTRODUCTION

There was a time not too long ago when businesses would think about business continuity only when a network server was down or when there was a theft or property damage from fire or flooding. Following September 11 and the more recent wide-spread disasters that have taken their toll on entire regions and weakened the economy, enterprises have been scrambling to bolster the public's confidence and implement adequate protective measures for their assets and operations.

In addition, businesses are facing increased pressure to adopt solid continuity and recovery programs. Failure to do so means overwhelming loss of time, productivity, incurred penalties, and loss of clients and profits. Many enterprises, in particular those such as call centers, online retailers, or those who provide products, services, and support around the clock must maintain a perpetual state of continuity preparedness or risk losing their customers to those who are better prepared.

This means that organizations can no longer rely on retrofit measures or patchwork damage control as the sole means of continuity planning. They must prepare proactively to make their continuity measures an *integral part of normal business* operations so critical functions can continue through emergencies and disruptions.

Furthermore, certain sectors such as the financial and healthcare industries must meet tougher compliance requirements and government mandates to serve all citizens and protect national interests.

A New Reality

With so much at stake, traditional continuity models fall far short of the daunting realities of a post 9-11 world. Increasingly widespread threats and security challenges call for a progressive approach based on a network model of collaboration for continuity. This means decentralized information sharing among all levels of government, private enterprises, and individual citizens.

Why a decentralized approach to information sharing?
Because, according to the Government Accounting Office (GAO), the United States now faces increasingly diverse threats from small states, groups, and individuals. These threats range from cyber attacks on critical infrastructure to terrorist incidents involving weapons of mass destruction or infectious diseases.

"Efforts to combat this threat will involve federal agencies as well as state and local governments, the private sector, and private citizens….the many organizations that will be involved in homeland security must have clearly articulated roles, responsibilities, and accountability mechanisms." (GAO-01-1158T)

Currently, we face major barriers to collaboration of efforts and information sharing. Key among these is an overriding organizational mindset that clings to outdated modes of approaching business continuity and disaster management.

But enterprises that seek to catapult business operations to the highest possible level—maintaining a customer base and public trust—must adopt a new, innovative approach to business continuity practices and thinking. This is true for both private and public entities.

The federal government in particular needs to dissolve resource silos and broadly disseminate information and standard guidelines across agencies and regions and to the private sector.

The Cold War model of closely guarded intelligence is "…ill-suited to today's challenges. The events of September 11, 2001, have starkly demonstrated the dangers associated with the failure to share information, not only within the federal government, but also between the federal government, on the one hand, and state

and local governments and the private sector on the other." (Markle Foundation, 2003)

So where do we go from here? This white paper presents some innovative approaches to business continuity and security that promise not only better business practices, but also savings and increased market value.

AN INNOVATIVE BUSINESS CONTINUITY MODEL

Employing a collaborative business approach using state-of-the-art tools and being part of a community-based network is essential to improving your organization's business continuity program and results in myriad benefits including the following:

- **Better awareness** (the first step toward change and transformation)
- **Better contribution** (the first step toward responsibility and accountability)
- **Better efficiency** (the first step toward lower total cost of ownership)
- **Better preparation** (the first step toward risk mitigation).

Awareness for Change and Transformation

The first and most critical step in establishing a robust, collaborative continuity program is building awareness. Decision-makers and leaders in the public and private sectors need to understand the value of a proactive, collaborative program that will enable them to work with all their stakeholders to quickly share information and coordinate operations before, during, and after an emergency.

The resulting speed and efficiency means that assets are protected, losses are minimized, and critical functions can go on so business and profits can be maintained.

Corporate culture and institutional thinking can be transformed only if decision makers enter the process early on and realize the benefits of investing time and resources in a holistic continuity program.

Buy-in and participation do not stop at the executive or leadership level. Vendors; financial, legal, and insurance partners; community organizations; and government agencies—among

others—are integral to the overarching security and continuity continuum and must work cooperatively to share resources and information during the planning, training and testing stages as well as through crises. Those who are not willing to work collaboratively will quickly fall behind and fail in the marketplace.

Why is collaboration so important? Because most organizations lack the tools, funds, and expertise to develop and implement a comprehensive continuity program that will effectively see them through a crisis. So developing strategic alliances and community partnerships provides access to a broad array of resources as well as critical information that may otherwise be missing within the boundaries of any individual enterprise.

Business leaders must go beyond seeing their continuity program as an extra overhead cost and accept it as a new and mandated way of doing business. This means embracing continuity planning and management as integral components of business operations that affect every-day decisions and tasks. Such tasks include legal and insurance decisions, staffing, data backup and storage practices, technology management, communications protocols, public relations, and more.

Contribution for Responsibility and Accountability

Continuity is best served with a network model of decentralized information accessible directly by users in both the public and private sectors. That's because key participants in disaster management and recovery are not found solely among top city officials. They are among those who work in the private sector including IT staff, emergency and rescue workers, healthcare providers, and personnel involved in an organization's day-to-day operations.

For example, if a widespread attack were to take place, response would occur at the local level first (municipal services, clinics, hospitals, even various professional service providers) before there would be time to call in national-level intervention.

However, an April 2003 GAO report indicated that many local areas and supporting agencies are inadequately prepared to respond to such an attack. Local officials reported varying levels of response capability and deficiencies in capacity, communication, coordination, and workforce shortages. And, more than two years after September 11, security and response efforts of public and private entities still lack a unified approach.

These preparedness issues were highlighted again recently during the national TOPOFF2 exercises of May 2003 where communication, coordination, and process were among the major problems that emerged during the disaster drills.

According to the final DHS report released in 2003, there were challenges identifying jurisdiction and authority channels. Even more troubling, there was no consistency for transmitting or receiving critical information and status updates. Furthermore, those who were not among the top officials were not well-informed and responsive enough in critical situations requiring immediate, decisive action. Private citizens were—for the most part—ill-prepared to take on their roles and responsibilities, leaving the door open for chaos, panic, and increased losses.

Yet experience has shown us that all participants in a continuity program are accountable for the success of the overall mission and are responsible for fulfilling their roles. Businesses must do their part to promote shared responsibility by all parties, and to track and assess progress toward the achievement of their security and continuity goals.

Meeting these goals demands collaborative training, planning, and tools that are accessible by all stakeholders.

Efficiency for Lower Total Cost of Ownership

Efficiency is an essential element of standard business practice and of BC planning and management. It helps eliminate redundancy as well as wasted time and resources. And, efficiency means more overall savings.

To achieve optimal efficiency, enterprises need the right resources, technology and processes. For example, collaborative software can help organizations process information, stay up-to-date, and monitor compliance. It could also provide real-time information for rapid mobilization, access from any location at any time, and checklists, contact information, etc. These are all elements that remove guesswork and errors from disaster management and recovery.

But technology for its own sake is not the answer. According to the most recent Markle Foundation report, an important element of the network is the interoperability of data sets and standards. We need to rely on commercially available exchange standards to gather and process information and then share that information across the business continuity network. And going even further,

we need directories that enable collaboration and sharing so that those in the network can easily manage vast amounts of information.

So process is the conduit by which resources (including people) and technology are managed for the greatest efficiency. An effective BCP program must have a built-in process for communicating within and outside of an organization; launching alternate business plans in case of emergency; and managing relief efforts, public relations, supply chains, personnel, legal and insurance services; and so forth.

The network model of collaboration speeds resource management, communications, and response to enable rapid and efficient recovery by taking resources and information out of the hands of a few and placing them with all relevant parties.

Preparation for Risk Mitigation

Currently, many organizations remain woefully unprepared to address their vulnerabilities. A recent survey by Logical Management Systems, Corp. and Cambridge Human Resource Group, Inc. reports that many businesses today still lack a business continuity program and an integrated crisis management plan.

Newsweek also reported, ”Since the fall of 2001, the Bush administration has spent or budgeted about $12.9 billion to prepare and protect the nation from a bioterror attack, including $5.2 billion in the budget for the 2004 fiscal year. But the recent reports of ricin-laced letters raise new concerns about how much better prepared we are now for such an assault.”

These reports are troubling in light of the growing threat of terrorist attacks and widespread disasters. Clearly, throwing money at the problem is not enough. If the national vision and approach don’t change, we will continue to face the same threats and vulnerabilities again and again with equally dismal and devastating results.

Continuity planning can no longer be a disjointed process of specialized or separate practices and elements such as threat assessment, facility relocation, disaster recovery, and so forth. All these specialties must come together under one plan that can be managed and monitored with collaborative tools, shared information and best practices.

A Role for Government

The federal government must do its part to enable the new network model and empower the private sector by tearing down information silos and sharing data and best practices regarding security threats and response measures.

In addition, the government must develop guidelines that protect private civil liberties so those in the private sector will be more willing to share privately-held information for national security purposes.

State and local officials are also demanding more guidance from the federal government on how to prepare for terrorist events, including biological warfare. There is a call for specific standards including details such as the appropriate size of response teams, assessing vulnerabilities toward food borne illness, and so forth.

This information, in turn, must be filtered to the private sector to enable nodes of preparedness and response at the front lines of defense including hospitals, community organizations, police and emergency call centers, and healthcare providers.

However, analytic tools are needed to sift through all the available information to determine what is critical, actionable information versus rumor and speculation.

Here, again, interoperable databases and technology can enable more individuals and organizations to participate in the security needs of their enterprises and their communities.

CONCLUSION

The new paradigm based on a collaborative network model requires broad commitment and resources. This new model "…consists not just of technological architecture, but also of the people, processes, and information that must go hand-in-hand with the technology, and the rules that govern how all of these elements interact." (Markle Foundation, 2003)

The traditional model of business continuity has failed us repeatedly as evidenced by the disruptions resulting from the 2003 Northeastern Blackout, the California wildfires, Hurricane Isabel and other more recent crises. We can no longer afford such a short-term view of our future and the resulting loss of lives and resources.

We need a new model and support tools designed for how we approach preparedness exercises at all levels, private sector involvement in emergency and continuity planning and recovery, and the sharing of innovative management decision tools that are effective, easy to use, and cost effective.

Today's businesses must adopt collaboration, network, and process survivability. These are the key governance requirements for both the private and public sectors of the future. And, the benefits to business and national security are immeasurable:

- Public trust
- Compliance with industry practices and government mandates (becoming increasingly necessary)
- Stakeholder confidence
- Increased market value
- Potential Savings
- Continuation of business operations
- Opportunities for improvement

ENABLING CONTINUITY WITH COLLABORATION

Is your BCP program all it could and should be to protect your business operations, your people, and your assets? How vulnerable are you to disruption. Do your plan and tools provide the following?

- ☐ Familiar, interoperable platform
- ☐ Shared workspace
- ☐ Template driven, team-based development capability
- ☐ Web-based and offline distribution options
- ☐ Ease of communication and information sharing
- ☐ Guided tools and templates to manage overall BCP program
- ☐ Easy training and consistency
- ☐ Plan development that enables consistency and efficiency
- ☐ Automatic access to plans by emergency teams
- ☐ Real-time tracking and notification
- ☐ Ability to deploy alternate business methods to continue business transactions
- ☐ Detailed archives of executed plans
- ☐ Integration with service and support program

If you are looking for collaborative tools and a consulting method that deliver powerful state-of-the-art BCP, emergency management and notification services, OpWatch™ offers the solutions and expert support you need to succeed.

ABOUT OPWATCH™ SERVICES

OpWatch™ is the consulting services division of Paradigm Solutions Corporation dedicated to business continuity and emergency response planning. Our team of experienced specialists shares a collaborative vision of continuity services that actively works with you to provide innovative services and consultation. And OpsPlanner™, our software suite built on a proven Microsoft® Windows 2003 and Windows Sharepoint Services platform, is easy to learn and integrates seamlessly into a familiar professional user desktop working environment.

The OpsPlanner™ collaborative approach takes the survival of critical assets out of the hands of a few and places it with all stakeholders—improving organizational awareness, accountability, and recovery. This team-based concept transforms plans and emergency management into efficient, integrated business continuity programs—providing benefits that far surpass those of traditional processes. Key features allow you to easily launch surveys, analyze data, exchange ideas and obtain plan approvals from any location.

OpWatch™ can help your organization:

- Build and manage comprehensive business continuity plans that you can access anywhere, any time
- Improve your organizational preparedness for all phases of planning, implementation, and management
- Increase organizational awareness through an easy-to-use Web interface
- Speed disaster recovery and reduce loss of staff, facilities, and data
- Maximize communication and efficiency during an emergency with real-time whiteboards and issue tracking
- Reach out to employees, customers, and suppliers during emergencies
- *Realize potential opportunities and savings.*

When you include OpWatch™ in your business continuity efforts, you ensure your organization's safety and success.

Endnotes

Government Accounting Office, GAO-01-1158T, "Homeland Security: A Framework for Addressing the Nation's Efforts." September 21, 2001.

Government Accounting Office, GAO-03-373, "Bioterrorism: Preparedness Varied Across State and Local Jurisdictions." April 7, 2003.

Government Accounting Office, GAO-03-715T, "Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues." May 8, 2003.

Government Accounting Office, GAO-03-924, "Hospital Preparedness: Most Urban Hospitals Have Emergency Plans but Lack Certain Capacities for Bioterrorism Response." August 6, 2003.

Markle Foundation, "Achieving a Networked Community for Homeland Security." 2003.

Newsweek, "Is the US Prepared for a Ricin-Type Attack?" February 5, 2004.

Security Industry Association, "Research Update," Vol. 1, Issue 12, 2003.

Sikich, Geary W., "Energy Surety?" 2003.

Sikich, Geary W., "Redefining Business Continuity for Uncertain Times." 2003.