Gartner Research

Publication Date: 23 July 2008 ID Number: G00159707

Business Continuity Management Defined, 2008

Roberta J. Witty

Business disruptions that turn into full-scale disasters with serious consequences have occurred frequently during the past 10 years. Planning is essential to ensure that organizational recovery and resiliency is cost-effective and sustainable. Use this research to assess your organization's ability to recover from a business interruption and increase the maturity of the business continuity management (BCM) program.

Key Findings

- The main drivers for BCM program growth and maturity — 24/7 service delivery, globalization and increasing operational risk — are expanding the scope of BCM beyond its roots in the IT department.
- The relationships among these three drivers are expanding the types of scenarios and the average outage duration being planned, as well as public/private sector coordination in recovery planning efforts, and are increasing the focus on satisfying government and industry regulations.
- BCM program components must apply globally across all locations, lines of business (LOBs) and workforces, with accommodations for local or functional issues, such as staff size at an operating location, locale-specific disaster scenarios and data center versus sales office.
- Crisis management must be an enterprisewide program.
- The HR and business operations aspects of workforce continuity are frequently overlooked in BCM planning.
- Except for the IT workforce, work area recovery options are not fully explored.
- Planning for pandemics is increasing in frequency.

Recommendations

- Perform a gap analysis for component coverage using the Gartner BCM components definition to uncover where your BCM program needs reinforcement.
- Expand the types of scenarios for which you plan and the outage time frame, to ensure that your organization can recover from local and regional disasters.

TABLE OF CONTENTS

LIST OF FIGURES

ANALYSIS

This document was revised on 25 July 2008. For more information, see the Corrections page on gartner.com.

1.0 Introduction

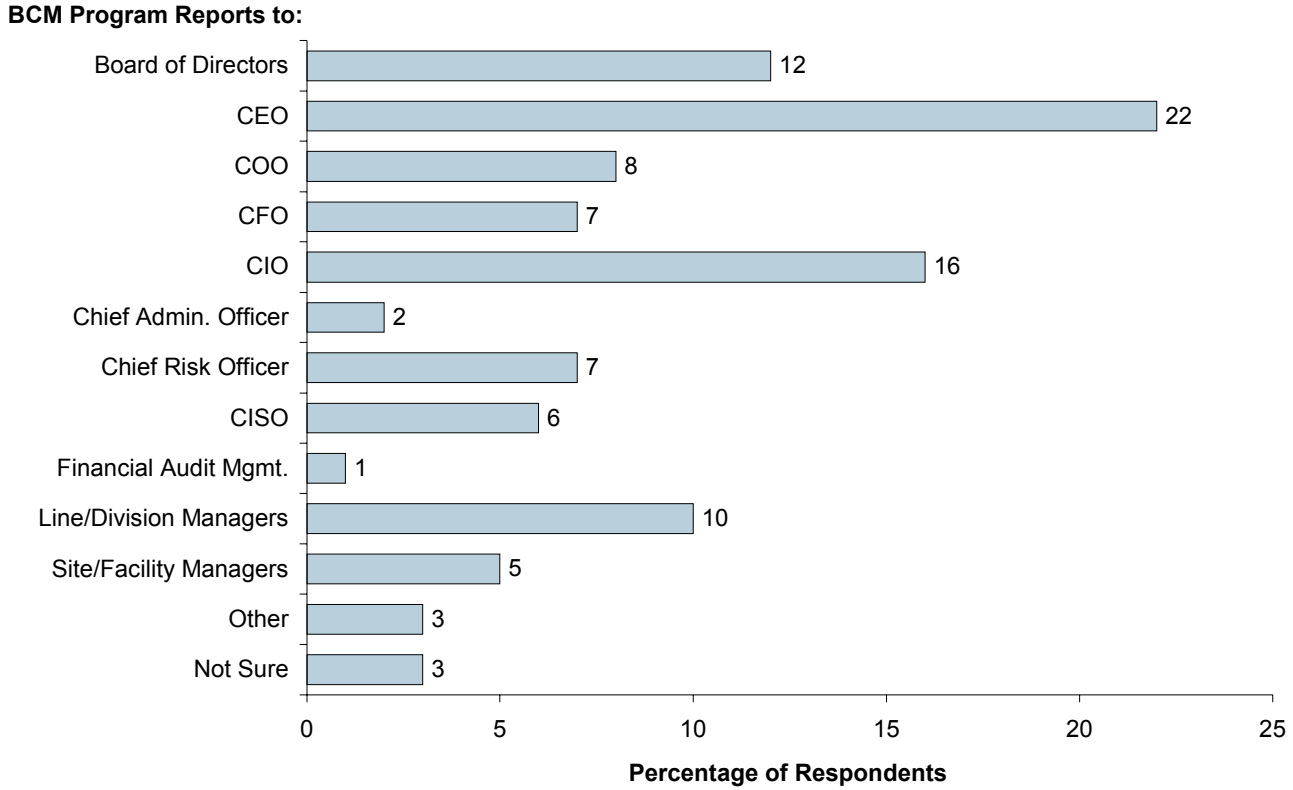
It is not a question of "if," rather one of "when" a disaster will strike your organization. Enterprises with the best BCM and IT disaster recovery (DR) practices have a corporate culture espousing availability and an understanding of the costs associated with business process outages. These enterprises also realize that following a well-defined process when disaster strikes is required to ensure business operations recovery (resulting in less downtime and costs). Conversely, trying to respond to an incident in crisis mode without the benefit of planning, coordination and testing will result in more downtime, high recovery costs due to "on demand" buying, and the complete lack of recovery resource availability — especially under regional disaster scenarios where many organizations, not just a single organization, are affected.

BCM is the practice of coordinating, facilitating and executing activities that ensure an enterprise's effectiveness in:

- Identifying and mitigating operational risks that can lead to business disruptions before they occur
- Responding to disruptive events (natural and man-made; accidental and intentional) in a manner that demonstrates command and control of crisis event responses by your organization
- Recovering and restoring mission-critical business operations after a disruptive event turns into a disaster
- Conducting a postmortem to improve future recovery operations

BCM is a comparatively new discipline for most enterprises, moving beyond IT DR's focus since the early 1990s on restoring IT systems and information assets to include *all* business operations and non-IT recovery activities. The political and social climate has changed, with entirely new classes of threats (for example, global terrorism) needing consideration in the BCM program. This and other types of operational threats, as well as changes such as 24/7 service delivery and business operations globalization, are expanding in scope and frequency, and the need for comprehensive, effective BCM is gaining senior-management-level visibility in the enterprise. This shift in visibility is evidenced in the results from the Gartner 2007 BCM Survey (see Figure 1). Enterprises that have mature BCM programs tend to be in high-risk, high-impact and often highly regulated vertical industries, such as financial services, telecommunications, healthcare, power generation and pharmaceuticals.

Figure 1. Survey Results, 2007: Reporting Structure in Companies With BCM Programs



Source: Gartner (2007)

Gartner receives inquiries from IT DR and BCM planners — often "lone rangers" with little authority and budget control in their enterprises — wanting to know how they can gain management commitment. These planners realize that senior management must understand the need for its involvement and support for a corporate sponsor and a BCM oversight committee. Several valuable options are available to gain senior management's support:

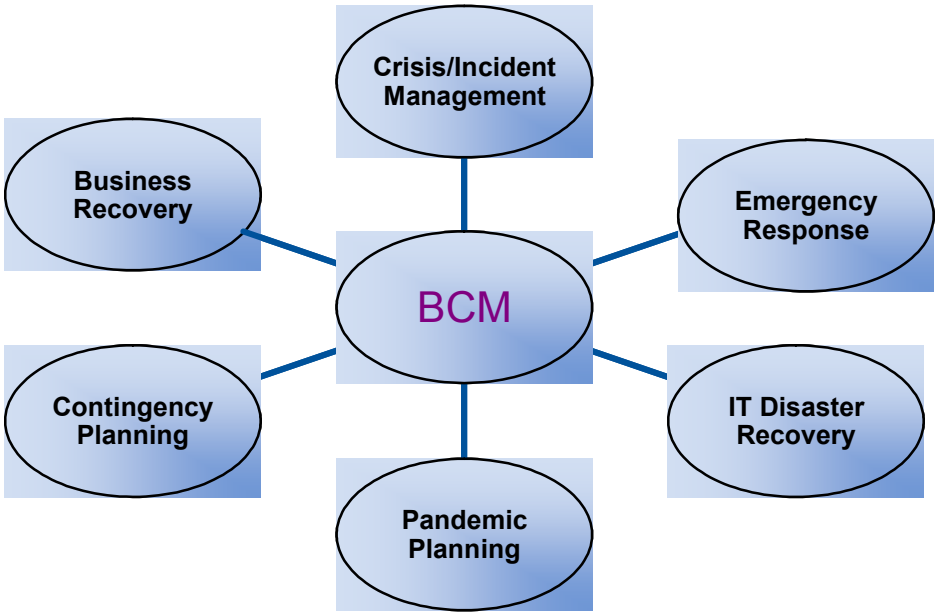
- Identify the impact on the organization of a business disruption and the value to the business of having a recovery program in place. The BCM oversight committee must communicate those results and value to senior management.
- Place responsibility for enterprisewide BCM at the top of the enterprise. Given the expanding risks covered by the BCM program, enterprise-level BCM responsibility is moving to the enterprise risk management office in organizations that have a culture of risk management.
- Apply BCM program components globally across all operating locations, LOBs and workforce, with accommodations being made for local or functional issues, such as staff size at an operating location, locale-specific disaster scenarios and data center versus sales office.
- Assign LOB-specific BCM responsibility in each business unit, with appropriate command and control links to the enterprise BCM program.

2.0 BCM Components

The transition from IT DR to BCM is recognition that IT services, which are essential for business operations, are just one component of a BCM program. To recover effectively from a disaster requires implementing risk mitigation before a disaster strikes, as well as planning for the recovery of all critical resources — IT department, workforce, facilities, vital records, equipment, suppliers, partners and service providers. Handling the non-IT aspects is often a more difficult job because it is primarily people- and process-oriented.

A successful BCM program includes the six components identified in Figure 2. Each component is comprised of specific activities.

Figure 2. BCM Components



Source: Gartner (July 2008)

2.1 Crisis/Incident Management

Crisis/incident management is comprised of the activities that the organization needs to take to manage and monitor the progression and response to all types of potential and actual business disruption events. These events include traditional BCM scenarios; reputation management crises, such as litigation, including class action lawsuits, product liability, labor disputes and discrimination charges; environmental issues; privacy breaches; identity theft and so forth. The goal is to ensure that the organization maintains its revenue, profitability, brand and reputation with its workforce, customers, markets and community as it reacts to and recovers from the interruption in its business operations. Crisis/incident management is dynamic, because the steps an organization takes to respond are dependent on the situational reality of the crisis.

Because crisis/incident management covers more than the traditional BCM scenarios, the function typically resides with the enterprise risk management group, the physical security office or directly in the president/CEO's office, rather than in the BCM office. In any crisis, the local workforce usually handles the response; however, given the reputation impact of a crisis and how the media can turn a small event into a global catastrophe, more organizations are requiring that all crisis/incident management activities should be coordinated through the enterprise crisis/incident management office.

The activities involved in crisis/incident management are:

- *Crisis command center/emergency operations center management and operations* is the process of establishing and managing the nerve center of any recovery event. In some organizations, the crisis command center is referred to as the "war room" (see "Toolkit: Requirements for Crisis Command and Emergency Operations Centers").
- *Crisis communications* is sent to all stakeholders (workforce, customers, suppliers, partners, shareholders, insurance companies and regulators), plus the public, to manage the fear, uncertainty and doubt that escalate during a crisis. Crisis

communications is a process of crafting public statements issued via the media (radio, TV, newspapers, advertisements, Internet news and so forth), as well as internal communications channels. The crisis communications process also includes crisis management team support activities, such as threat monitoring and media monitoring.

- *Emergency notification* is sent to the workforce, as well as to other selected stakeholders, often through automation to endpoints such as cell phones, land lines, e-mail, Short Message Service (SMS), physical alerting systems, kiosks, desktops and so forth (see "Emergency Notification Planning," "How to Quickly Spread the Word Locally: Basic and Advanced Editions" and "Automated Emergency Notification Will Speed Disaster Recovery").

- *Law enforcement coordination,* especially in regional disasters, is a vital part of every recovery effort. In most cases of an operational risk being exploited, the organization does not control its destiny during the initial hours and relies on local authorities for key decision making, such as when the organization can return to a facility, when it has to investigate the cause of an event because there is potential foul play or more than one organization is involved and so forth (see the government-focused recommended reading list).

2.2 Emergency Response

Emergency response is comprised of the activities that are directly involved with the physical aspects of the disaster and the determination of the scope of the disaster, such that a decision is taken to execute a recovery plan or issue a stand-down notice. The activities involved in emergency response are:

- *Damage control and assessment* of the facility is done by facilities management teams along with the property owners, and fire, gas and police departments. If there is an accident, for example, at a physical plant in a chemical manufacturing site, then hazardous materials (hazmat) teams may be required to investigate and respond to the incident.

- *Ensuring life and safety* of the workforce, as well as others in the facility at the time of the event, is done to provide immediate medical attention and rescue operations following an event.

Also, see the government-focused recommended reading list.

2.3 IT Disaster Recovery

- IT disaster recovery management (DRM) is comprised of the activities that ensure that the data center and all IT services are recovered according to business expectations. The activities involved in IT DRM are:

- *Network recovery* is the starting point — a Tier 0 — of any IT recovery effort

- *Hardware recovery* — including servers, storage, routers, switches, gateways and so forth — for essential IT services

- *Desktop recovery,* for the recovery workforce, including IT personnel and business recovery team members

- *Software recovery* including utilities, operating systems, databases and applications, whether they are housed internally or externally to the organization

- *Data recovery* associated with essential IT services stored in file servers, databases and so forth
- *Telecommunications recovery,* including voice and data
- *Information security recovery,* including encryption keys, shared/service account passwords, authentication tokens and so forth

Also, see the IT DR recommended reading list.

2.4 Business Recovery

Business recovery is comprised of the activities that support the recovery of essential business processes. Business recovery plans, in most cases, point to an IT DR plan that addresses the needs of that particular LOB. The activities involved in business recovery are:

- *Knowledge management* support is a set of risk mitigation controls — such as FAQ databases, cross-training personnel and so forth — that are put in place prior to a disaster and then used or implemented during a recovery.
- *Business resumption* comes into play during the first few hours of a disaster when IT is not available as normal, but the enterprise still needs to conduct business, albeit at a reduced rate. Business resumption only lasts until IT has recovered the essential IT services for the LOB. Examples of business resumption plans include:
  - Having a message play at the call center directing customers to call back in 30 minutes
  - Using a laptop and a spreadsheet to manage transactions
  - Sending orders via fax or e-mail rather than on the Web site
- *Work area recovery* is the process of securing alternate work space for the workforce to use following the disaster. There are many options: work at home, third-party service providers, mobile units, hotel ballrooms and so forth.
- *Workforce continuity* addresses the human aspect of recovery — the people who run the business in the recovery process — not just the provision of access to IT resources. There are three goals of workforce continuity: maintaining the social networks of the workforce, preserving the organization’s reputation as an employer and a member of the local community, and enhancing the recovery of the organization because the enterprise's personnel are taken care of prior to, during and after a disaster. Some lesser-addressed risks around workforce continuity include: handling staff outages due to school closings and elder care support, as well as addressing the identity management practices that support emergency access setup for workforce members taking on different roles during a crisis.
- *Records management* is the process that identifies and protects the enterprise's vital records, including paper-based and electronic information.
- *Supply chain recovery* is a new area for BCM, but one that is critical as enterprises decentralize and globalize their businesses. It includes looking at the overall supply chain process for each product or service the organization offers, and establishing controls prior to disaster risk mitigation. Supply chain recovery activities work in conjunction with the contingency planning component of BCM. Examples of disaster risk mitigation controls are:

- Having two vendors, rather than one vendor, supply raw materials
- Revamping manufacturing production so that two manufacturing sites can support the other if one is offline
- Understanding transportation practices and implementing rerouting procedures to divert goods from the failed facility to a working one
- Creating agreements with unions to allow a nonunion-supported trucking firm into a working facility if it is under different union control from the failed facility and so forth

- *Business interruption insurance* is part of property and casualty insurance coverage and is a risk transference control. Choose your outage time frame carefully, and then secure a policy that covers that time frame, because an enterprise will be unable to recover expenses incurred during a disaster if the event lasts longer than the policy's time frame.

2.5 Contingency Planning

Contingency planning addresses the risks associated with the external operations of the organizations that may cause a business disruption to your organization, which has no internal failure of its own. The activities involved in contingency planning are:

- *Outsourcing* can introduce new or additional risks into the organization because the service provider is in a different location. Therefore, the service provider has a different natural disaster or biohazard profile, may be a more public or more sensitive organization and, therefore, more prone to terrorist attacks or civil unrest, does not follow IT and information security best practices to the same level as the organization at risk and so forth. Understanding the organization's complete supply chain — internal and external — is required to mitigate risks prior to their being exploited, as well as responding to them when they are not related directly to the organization.
- *Raw materials supply management* — whether for physical goods, services such as electric power or telecommunications, or external workforce skills — must be reviewed to see if there is a single point of failure in this portion of the supply chain. Putting in place additional supplies, or contracts for day-to-day production or recovery time, are two solutions.
- *Community* presence of government agencies, organizations with divergent social or political views and so forth can affect an enterprise's ability to continue business operations as usual, if one of the organizations experiences a disruptive event and prevents the enterprise from inhabiting any of its facilities. The BCM program requires that an enterprise surveys its own neighborhood, identify potential external community participants, and then build response and recovery plans for such an event.

2.6 Pandemic Planning

Most businesses are not prepared for a pandemic outbreak (for example, influenza) and have failed to heed earlier warnings, because many think that a pandemic event will never happen, or they figure it's no use because they will be shut down anyway. The IT organization can only address a few of the changes that businesses need to make to be better prepared. Most changes will occur in the business processes (see the pandemic planning recommended reading list).

Pandemic planning coordination often is seen as the responsibility of the BCM team because it has the project management skills, as well as the business and IT process knowledge, to coordinate such a planning effort. Although the BCM team may have this responsibility, pandemic planning efforts are more extensive than traditional BCM

The key components of BCM that will be critical during a pandemic event are crisis/incident management and business recovery, especially supply chain recovery and workforce continuity. The workforce will not be relocating to recovery sites if they won't go to the fully functioning production site (see Note 1).

3.0 BCM Component Examples

Figure 3 provides examples of disruptive events and appropriate solutions that each BCM component addresses.

Figure 3. Business Continuity Component Examples

	Emergency Response	IT Disaster Recovery	Business Recovery	Contingency Planning	Pandemic Planning
Objective	Physical operating facility	Mission-critical applications	Mission-critical business processing	External partners, suppliers	Workforce absentee rate of 40% or more
Focus	Site outage or damage	Partial or complete outage at data center	Site or regional outage	External event forcing internal disruption	Pandemic
Deliverable	Emergency response plan	IT disaster recovery plan	Business recovery plan	Business contingency plan	Pandemic management plan
Sample Events	Earthquake, fire, flood	Data center fire or power outage	Electrical outage in sales office	Supplier fire at manufacturing facility	Avian Flu epidemic
Sample Solution	Site damage assessment; search and rescue	Recovery data center 150 miles away	Recovery site in different power grid; work at home	Backup supplier	Work at home; shift work out of region; shut down
Crisis/Incident Management Crisis command center (physical/virtual), crisis communications and emergency notification plans					

Source: Gartner (July 2008)

4.0 Applying the Gartner BCM Components Into the Organization

The following steps should be taken to ensure that your BCM program encompasses all the Gartner BCM components:

1. Perform a gap analysis for component coverage using the Gartner BCM components definition to uncover where your BCM program needs reinforcement.
2. Put in place a governance structure to oversee the enterprisewide BCM program.
3. Assign BCM responsibility to senior management in the organization and in each LOB.
4. Align IT DR with BCM for an integrated approach.

5. Expand the types of scenarios for which you plan and the outage time frame, to ensure that your organization can recover from local and regional disasters.
6. Assess your internal and external business interruption risks on a quarterly basis and plot them to your enterprise's risk register.
7. Establish an enterprisewide crisis/incident management office reporting as close to the president's or CEO's office as possible. Establishing the office as an enterprisewide program ensures that local business interruptions are managed to the benefit of the entire enterprise.
8. Establish a crisis communications strategy, plan and communiques before a crisis occurs.
9. For each of your operating locations, establish BCM program links to local, county, state/province, country and international law enforcement and utilities.
10. The BCM program office must work with the physical security department because the latter often has primary responsibility for all facility and life/safety issues.
11. Befriend the media in each of your operating locations.
12. Perform a mapping of all business processes to their associated facility, IT department, workforce, vital records, special equipment needs and so forth to ensure that all needed assets are identified and addressed in the recovery plan.
13. Put in place a workforce continuity program that includes HR, business operations and IT components.
14. Establish business resumption plans for all mission-critical business processes. Be sure to consider less-automated and manual procedures as part of the recovery plan.
15. Ensure that you have work area recovery space for all business and IT personnel that can take you through your longest outage duration time frame.
16. Establish a records management program to identify all vital records — electronic and nonelectronic.
17. Establish a supply chain recovery program to ensure that recovery from outages at raw materials suppliers and key service providers are addressed in your recovery plans.
18. Review and upgrade your business interruption insurance policy to ensure that it covers the longest outage duration being planned, based on your recovery scenarios.
19. Participate in all private/public partnerships available in all operating locations.
20. Start pandemic planning today.

RECOMMENDED READING

BCM

"Gartner for IT Leaders Overview: The Business Continuity Manager"

"Toolkit: Job Description for Business Continuity Manager"

"Enlightening the CEO on Business Continuity Management"

"Top-Five Issues and Research Agenda, 2008: The Business Continuity Manager"

"Hype Cycle for Business Continuity Management, 2008"

"Toolkit: Requirements for Crisis Command and Emergency Operations Centers"

"Best Practices for Conducting a Business Impact Analysis"

"New York Projects Show Critical Need for Unified Emergency Management"

"Hurricane Katrina Highlights Need for Disaster Preparedness"

"Hurricane Katrina Presents a True Test of Disaster Recovery for Insurers"

"Building Business Continuity Planning Into Every IT Project"

"Toolkit: Best Practices for a Successful Tabletop Recovery Test"

"Business Continuity Questions From European Midsize Businesses"

Financial Services Industry Focused

"Managing Scarcity-Driven Business Disruptions"

"Catastrophic Risks Are Real for Health Insurers"

"Banking and Investment Services BCM/DR, 2006"

"Catastrophic Events Will Continue to Test Insurers Through 2012"

"New U.S. Guidance on IT in Pandemics"

Government Focused

"The Emergency Services Sector of the National Infrastructure Protection Plan"

"Emergency Communications Managers Should Plan at the National Level Because of the Nature of Voice Over IP Services and Regulations"

"Governments Working Together Bridge Emergency Response Gaps"

"Emergency Notification Planning"

"Management System Unites U.S. Emergency Response Groups"

"New York Projects Show Critical Need for Unified Emergency Management"

"How to Quickly Spread the Word Locally: Basic and Advanced Editions"

"Automated Emergency Notification Will Speed Disaster Recovery"

"Miami-Dade Launches Multijurisdictional Government Contact Center"

"Governments Are Using IT to Better Secure the Homeland"

"Case Study: City of Chicago and ChicagoFIRST Public-Private Partnership"

IT DR

"How to Conduct a Disaster Recovery Management Self-Assessment"

"Toolkit Decision Framework: Best Data Center Locations for Disaster Recovery"

"Disaster Recovery Spending Trends"

"Toolkit Best Practice: Disaster Recovery Service Levels: What Makes Them Different and Why They Are Important"

"Toolkit: Disaster Recovery Contract Negotiating Points"

"Toolkit Best Practices: How to Benchmark Your Disaster Recovery Processes"

"How to Organize for Disaster Recovery Management"

"Cost Cutting Disaster Recovery in 2008"

"IT Service Dependency Mapping Tools Provide Configuration View"

Pandemic Planning

"New U.S. Guidance on IT in Pandemics"

"Prepare Now for a Coming Avian Influenza Pandemic"

"Key Steps to Prepare for a Possible Avian Influenza Pandemic"

"Pandemic Investing"

"Prepare for Avian Influenza: Our Interview With Andre Greyling, CIO, Hong Kong Hospital Authority"

"More 'Key Steps to Prepare for a Possible Avian Influenza Pandemic'"

"Prepare for Avian Influenza: Our Interview With the World Health Organization's Dr. David Nabarro"

"Prepare for Avian Influenza: Our Interview With Microsoft's Jeff Jones"

"Dell CEO Highlights Preparations Needed for Avian Influenza"

"Prepared for Avian Influenza: Our Interview With T. Rajah, CIO, CLSA"

"Business Applications Can Minimize Operation Discontinuity Created by Avian Flu"

"SARS: The First Global Crisis of the 21st Century"

"Scenarios for Avian Influenza and How IT Can Mitigate Risk"

Acronym Key and Glossary Terms

BCM business continuity management

DR disaster recovery

DRM disaster recovery management

LOB line of business

SMS Short Message Service

VPN virtual private network

Note 1.
Pandemic Planning Guidance

The following advice is provided to jump-start your pandemic planning initiative:

- Use scenario planning (low, medium or high impact) to build your plans now. If you wait for an outbreak, then it will be too late to overcome the pandemic crisis. Service providers will not be able to address your organization's needs during times of crisis.
- Do not build plans addressing the response to a pandemic on competitive instincts. Rather, ensure that the plans are collaborative and supportive in nature.
- Start honest, rigorous, inventive, ongoing and documented testing immediately to isolate and remediate problem areas.
- Establish a succession plan for the loss of key personnel throughout the organization.
- Ensure that IT and business managers worldwide identify critical operation skills shortages and initiate staff cross-training, testing and certification. This requires the longest lead time and is the most disruptive of the improvements.
- Determine realistic business operations sustainability and the likely downtime for IT staff absentee rates of 10% through 50%, with various combinations of leaders and skilled staff. Do not expect heroic devotion.
- Educate your workforce on personal hygiene issues.
- Work with public health and other government agencies.
- Plan for loss of travel and transportation, and reduced food supplies.
- Implement more work-at-home options — for example, virtual private network (VPN) access and videoconferencing. Expanding VPN access now is a critical move because once the World Health Organization raises the alert level from three to four, organizations may be challenged to secure additional bandwidth from their service providers, because everyone will be in panic mode and the service providers may not be able to respond as quickly as needed.
- Look to external parties in advance to provide skills where appropriate.
- Stagger the workforce work schedule into shifts.
- Work with customers and partners to minimize any disruption by developing coordinated crisis-response capabilities.
- Prepare for privacy protections reduction — for example, tracking sick people and travelers.
- Review where your business might have spare capacity as a result of the pandemic impact and see where else it can be used.
- Review business continuity and DR plans to determine where and when they can be used.
- Stockpile critical supplies and raw materials — just-in-time inventories won't work.

- Use more online systems — for example, order taking, training, FAQs and knowledge bases.

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509

Gartner