

BUSINESS SURVIVAL™

A Business Continuity Newsletter for Decision-makers from ROTHSTEIN ASSOCIATES

Volume 8, Issue 2

Copyright 2006, Rothstein Associates Inc.

CONTENTS

- *Making Plans for an Influenza Pandemic*
- *Trends in IT Outsourcing Continue in the U.S.*
- *IBM's Web Service Level Agreements (WSLA) Project*
- *News*
- *Upcoming Events*
- *Recommended Reading*
- *News*

MAKING PLANS FOR AN INFLUENZA PANDEMIC

With all the “chatter” going on regarding a potential influenza pandemic, many experts are offering their recommendations on how to deal with this threat. **BUSINESS SURVIVAL** has been searching various resources, and we’ve identified two that should be of interest to you. The first is the Centers for Disease Control (CDC), a name most of you already know. The second is Protective Countermeasures & Consulting, which is probably a new name for you. PCC is an advisory services firm based in New Rochelle, NY that specializes in security, counter terrorism, and crisis management. **Business Survival** is pleased to offer you pandemic planning guidelines from the CDC, and a list of questions regarding pandemics from Protective Countermeasures.

The first selection is from the CDC’s Business Influenza Pandemic Planning Checklist. Obtain further information at www.pandemicflu.gov and www.cdc.gov/business.

Plan for the impact of a pandemic on your business

1. Identify a pandemic coordinator and/or team with defined roles and responsibilities for preparedness and response planning. The planning process should include input from labor representatives.
2. Identify essential employees and other critical inputs (e.g. raw materials, suppliers, subcontractor services, products, and logistics) required to maintain business operations by location and function during a pandemic.
3. Train and prepare ancillary workforce (e.g. contractors, employees in other job titles/descriptions, retirees).
4. Develop and plan for scenarios likely to result in an increase or decrease in demand for your products and/or services during a pandemic (e.g. effect of restriction on mass gatherings, need for hygiene supplies).
5. Determine potential impact of a pandemic on company business financials using multiple possible scenarios that affect different product lines and/or production sites.
6. Determine potential impact of a pandemic on business-related domestic and international travel (e.g. quarantines, border closures).
7. Find up-to-date, reliable pandemic information from community public health, emergency management, and other sources and make sustainable links.
8. Establish an emergency communications plan and revise periodically. This plan includes identification of key contacts (with back-ups), chain of communications (including suppliers

and customers), and processes for tracking and communicating business and employee status.

9. Implement an exercise/drill to test your plan, and revise periodically.

Plan for the impact of a pandemic on your employees and customers

1. Forecast and allow for employee absences during a pandemic due to factors such as personal illness, family member illness, community containment measures and quarantines, school and/or business closures, and public transportation closures.
2. Implement guidelines to modify the frequency and type of face-to-face contact (e.g., hand shaking, seating in meetings, office layout, shared workstations) among employees and between employees and customers (refer to CDC recommendations).
3. Encourage and track annual influenza vaccination for employees.
4. Evaluate employee access to and availability of healthcare services during a pandemic, and improve services as needed.
5. Evaluate employee access to and availability of mental health and social services during a pandemic, including corporate, community, and faith-based resources, and improve services as needed.
6. Identify employees and key customers with special needs, and incorporate the requirements of such persons into your preparedness plan.

Establish policies to implement in a pandemic

1. Establish policies for employee compensation and sick leave absences unique to a pandemic (e.g., non-punitive, liberal leave), including policies on when a previously ill person is no longer infectious and can return to work after illness.
2. Establish policies for flexible worksite (e.g. telecommuting) and flexible work hours (e.g., staggered shifts).
3. Establish policies for preventing influenza spread at the worksite (e.g. promoting respiratory hygiene/cough etiquette, and prompt exclusion of people with influenza symptoms).
4. Establish policies for employees who are exposed to pandemic influenza, are suspected to be ill, or become ill at the worksite (e.g., infection control response, immediate mandatory sick leave).
5. Establish policies for restricting travel to affected geographic areas (consider both domestic and international sites), evacuating employees working in or near an affected area when an outbreak begins, and guidance for employees returning from affected areas (refer to CDC travel recommendations).
6. Set up authorities, triggers, and procedures for activating and terminating the company's response plan, altering business operations (e.g., shutting down operations in affected areas), and transferring business knowledge to key employees.

Allocate resources to protect your employees and customers during a pandemic

1. Provide sufficient and accessible infection control supplies (e.g., hand-hygiene products, tissues and receptacles for their disposal) in all business locations.
2. Enhance communications and information technology infrastructures as needed to support employee telecommuting and remote customer access.
3. Ensure availability of medical consultation and advice for emergency response.

Communicate to and educate your employees

1. Develop and disseminate programs and materials covering pandemic fundamentals (e.g., signs and symptoms of influenza, modes of transmission), personal and family protection and response strategies (e.g., hand hygiene, coughing/sneezing etiquette, contingency plans).
2. Anticipate employee fear and anxiety, rumors and misinformation and plan communications

- accordingly.
3. Ensure that communications are culturally and linguistically appropriate.
 4. Disseminate information to employees about your pandemic preparedness and response plan.
 5. Provide information for the at-home care of ill employees and family members.
 6. Develop platforms (e.g., hotlines, dedicated websites) for communicating pandemic status and actions to employees, vendors, suppliers, and customers inside and outside the worksite in a consistent and timely way, including redundancies in the emergency contact system.
 7. Identify community sources for timely and accurate pandemic information (domestic and international) and resources for obtaining counter-measures (e.g., vaccines and antivirals).

Coordinate with external organizations and help your community

1. Collaborate with insurers, health plans, and major local health care facilities to share your pandemic plans and understand their capabilities and plans.
2. Collaborate with federal, state, and local public health agencies and/or emergency responders to participate in their planning processes, share your pandemic plans, and understand their capabilities and plans.
3. Communicate with local and/or state public health agencies and/or emergency responders about the assets and/or services your business could contribute to the community.
4. Share best practices with other businesses in your communities, chambers of commerce, and associations to improve community response efforts.

The second selection is excerpted from **Protective Countermeasures & Consulting's Influenza Pandemic Planning Questionnaire** (Copyright 2006 by Protective Countermeasures & Consulting. Reprinted with permission). Obtain further information at www.protectivecountermeasures.com.

Planning for a Pandemic - General

1. Have you developed a pandemic response plan?
2. Have you created a pandemic response team?
3. Do the team members have clearly defined roles?
4. Have you exercised your plan?
5. Have all areas of your business been included in the planning process?
6. Are all levels of your workforce included in the planning process?
7. Are OSHA guidelines referenced or addressed in your planning?
8. Have multilateral health organizations been consulted, e.g., CDC?
9. Have your plans been approved by corporate management?
10. Do your plans incorporate the latest available information?
11. Have you addressed individual department plans?
12. Are you in a multi-tenant facility or a self-contained facility (risk of infection is greater in a multi-tenant facility)?
13. Have you established recovery plans for technology and systems?
14. Have you established recovery plans for mission-critical business units?
15. Who is in your chain of command?
16. Who in the chain of command can declare a pandemic response?
17. Who can substitute for this person if he/she is ill?
18. Have you established a plan for contacting family members and/or employees away from the organization (at home, on vacation, etc.)?
19. Have you considered the operational and economic impact of a pandemic?
20. Have you evaluated your budget in accordance with pandemic planning?

21. Do you have multiple copies of your plan?
22. How will supplies and essential products be delivered to employees at a recovery site?
23. Does your plan provide for logistical support (food, beverages, etc) for pandemic teams?
24. Does your plan assign operational support for the Pandemic Response Team?
25. Does your plan indicate the location of the EOC?
26. Does your plan provide for a backup EOC site?
27. Does your plan provide transportation to the backup EOC site?

Policy Issues in a Pandemic Incident

1. Have you incorporated plans for the rapid recruitment of additional workers?
2. Does your staff know who to report incidents to?
3. Does your response plan support telecommuting?
4. Does your plan consider employee compensation?
5. Have you considered employee sick leave or other absences?
6. Does your plan also consider family issues?
7. Does your plan consider PR before/after the crisis?
8. Does your plan identify a line of succession for key positions at the facility?
9. Do employees understand their roles and responsibilities in a pandemic response plan?
10. Does your plan identify how to implement resource controls?
11. Does your plan identify how to preserve essential records?
12. Does your plan provide for the backup of essential records at an offsite location?
13. Does your plan identify a specific team member responsible for monitoring the effects of the pandemic on the facility?
14. Does your plan identify a specific team member responsible for reporting the effects of the pandemic on the facility?
15. Does your plan identify a specific team member responsible for documenting an event log regarding the effects of the pandemic?

Protecting Employees During a Pandemic

1. Do you encourage staff to receive flu shots?
2. Do you provide funding to pay for employee annual flu shots?
3. Can your company provide flu shots on site?
4. Do you have sufficient medical supplies for key staff, e.g., vaccines, masks, antivirals, gloves?
5. Do you have proper sanitizing equipment?
6. Do you have hand sanitizers in common areas?
7. Does your facility have an evacuation procedure?
8. Does your plan indicate who is responsible for issuing evacuation/quarantine orders for the facility? When they should be issued?
9. Do your evacuation procedures work in conjunction with neighboring businesses?

TRENDS IN IT OUTSOURCING CONTINUE IN THE U.S. From the Data Center Journal

Offshore outsourcing of IT has not gone away as many had hoped. Even though the amount of offshore work remains relatively small, given the size of the industry, several analyst studies are predicting a sharp rise in offshore development. The result is that the trends are getting a lot of attention. This attention has many debating the pros and cons.

Recently, during President Bush's State of the Union address, it was clear that the administration

wants to develop an economic climate that creates jobs in the U.S. However, there appear to be no major policies that would prevent outsourcing of any kind, including IT. It would appear that the administration, like many of us, does not have a clear picture to what the impact will be to the IT industry in particular.

Congress and the Bush administration could have an effect on offshore work in a number of ways: 1) by using their power over regulated industries, such as financial services, to push companies to keep jobs in the U.S.; 2) by passing legislation that sets “buy American” standards for federally purchased IT products; and 3) by raising national security issues. The U.S. General Accounting Office is already examining some of those issues.

Recently GM began outsourcing their IT requirements to several services providers such as IBM and EDS. This deal has been described as the largest commercial contract bidding process in the history of the tech industry. Many fear that this will become the new IT model. It is unclear, however in this particular outsourcing example as to how much will be sent offshore.

Companies that outsource just because “everybody is doing it” may be surprised by unexpected costs and complications. About one-half of the outsourcing arrangements are terminated, for a variety of reasons. Some new overseas vendors encounter financial difficulties or are acquired by other firms with different procedures and priorities.

Businesses that arbitrarily set a fixed percentage of work to be outsourced likely will regret it. Newcomers to overseas contracting may find themselves dealing with unreliable suppliers who put their work aside when they gain a more important client or their overseas vendor may suffer rapid turnover of skilled employees who find jobs with more desirable firms. Typical Indian operations in business processing — including call centers and offices handling payroll, accounting, and human resources functions — often lose 15-20 percent of their work forces each year. While software-programming skills are plentiful in some parts of Asia, good managerial experience is very limited.

Furthermore, overseas managers often do not understand the American business environment — our customers, lingo, traditions, and high quality control and expectations for prompt delivery of goods and performance of services. Dell moved its call center support for corporate business from India back to the United States in 2003. Its clients had complained about foreigners speaking English in hard-to-follow accents and giving vague answers to technical questions. Given the continued flow of complaints from individual customers, we may wonder what further pullbacks may occur.

Source: Data Center Journal

Copyright ©2006, Bob DeCoufle.

Reprinted with permission from EDM2R Enterprises, Inc.

All Rights Reserved by the original copyright holder.

www.datacenterjournal.com

IBM'S WEB SERVICE LEVEL AGREEMENTS (WSLA) PROJECT

The Web Service Level Agreement (WSLA) project, developed by IBM, addresses service level management issues within a Web services environment. Issues addressed include SLA specification, creation and monitoring. The project provides

- Explicit specifications of service level agreements that can be monitored by the service provider, customer and even by a third-party;
- Ease of SLA creation using template-based authoring tools; and

- Distributed monitoring framework for deployment in a single site or across multiple sites by translating SLA data in configuration information for the individual service provider components and third party services to perform the measurement and supervision activities.

The WSLA creation and monitoring framework complements various other projects addressing issues on proactive management of a service environment, e.g., provisioning resources, workload management, etc., according to the agreed upon service levels specified via WSLA. For more details on the WSLA project, visit the project home page on <http://www.research.ibm.com/wsla/>.

RECOMMENDED READING

These and hundreds of other books, software tools, videos and research reports are available from [THE ROTHSTEIN CATALOG ON DISASTER RECOVERY](http://www.rothstein.com) and [THE ROTHSTEIN CATALOG ON SERVICE LEVEL MANAGEMENT](http://www.rothstein.com) at www.rothstein.com. Contact info@rothstein.com to order:

Human Error: Causes and Control

by George A. Peters and Barbara J. Peters

“Human Error is regularly viewed as an inevitable part of everyday life. In many cases the results of human error are harmless and correctable, but in cases where injury and death can occur, reduction of error is imperative. An integration of useful how-to-do-it information, **Human Error: Causes and Controls** covers theories, methods, and specific techniques for controlling human error.”
2006, 214 pages, Order #DR786.

Risk: Assess, Mitigate, Protect (DVD)

Featuring Barry Pruitt and Michael Herrera, CBCP

“How to assess threats to your organization, know your level of mitigation, and when/where to spend limited monies for protection. Learn key definitions; how to identify applicable threats and mitigating controls; and write winning risk event statements. You’ll learn the pitfalls — and gain insight — for presenting the risk assessment to executives. As a professional, you need proven risk approaches as one of the cornerstones of your BCP program, and the confidence to apply it to your organization.”
2006 (four DVDs), Order #DR785.

Emergency and Backup Power Sources: Preparing for Blackouts and Brownouts

by Michael F. Hordeski, P.E.

“This book provides invaluable information on emergency and backup power sources, an issue that continues to gain significance as we experience an aging power distribution system that often fails to provide reliable power. The massive power outage in the summer of 2003 that affected eight states and parts of Canada is one example. The reader will find much useful information on the types of systems that can take over during power interruptions, such as standby power systems that employ batteries, kinetic energy storage, fuel cells, reciprocating engines, and turbines.”
Topics include power disturbances and interruptions, spikes and noise, sags and surges, blackouts and brownouts, surge suppression, voltage regulation, load management, power quality issues, reliability and maintainability, comparison of operating costs, environmental issues, blackout planning, emergency procedures and more.”
2005, 313 pages. Order #DR787.

NEWS

Business Continuity Tests Announced for U.S. Financial Markets

The U.S. Securities Industry Association has written to SIA Managing Executives regarding an industry-wide business continuity test scheduled for Saturday, October 14, 2006. SIA is leading the test, along with The Bond Market Association, The Futures Industry Association and the Financial Information Forum, as part of the ongoing securities industry testing initiative. The 2006 test will be similar to the one conducted on October 15, 2005, and includes additional payment and market data components. SIA said that the test would not simulate an outage in any specific geographic area. Instead, all firms will connect simultaneously from their backup business and technology sites to the markets and utilities. SIA will compile aggregate results, but will not reveal the individual performance of any organization. For more information go to http://www.sia.com/business_continuity/

ACP Publishes Member Comments on Hurricane Katrina

The Association of Contingency Planners has published a white paper that compiled member thoughts and recommendations regarding the response and preparedness measures surrounding Hurricane Katrina. The document culminates the ACP's recent polling of its membership to provide their unique perspective on the event. Download the document at http://www.acp-international.com/articles/ACP_Hurricane_Katrina_Observations.pdf

2006 Business Continuity Expo in London

Now in its third year, Business Continuity - The Risk Management Expo 2006 will be held March 15-16 at the ExCel in London. This year's event is a key part of Business Continuity Awareness Week (UK and Europe), scheduled for March 13-19. The Risk Management Expo will be held alongside Technology for Compliance, a conference that addresses issues of regulatory compliance and corporate governance. The combined conferences focus on three key areas of risk management: continuity, security and compliance. Among the featured speakers are Richard Armour, IT Director, Dell, Inc; Victor Meyer, Global Head of Business Continuity Management, Deutsche Bank; Chris Keeling, Head of Crisis Management, Barclays Bank; Richard Maddison, Deputy Head of Business Continuity, Financial Services Authority; Kevin Stirzaker, Continuity & Risk Assurance Manager, Vodafone; and Geoff Dunmore, Operational Security Manager, London Underground. Well over 100 exhibitors are expected at the event. The event is produced by IMP Events; for more information on the event and to register for free expo tickets, visit www.businesscontinuityexpo.com.

2006 Business Continuity & Corporate Security Conference in New York

The annual Flagg Management conference on business continuity and security will be held in New York City on March 21-22, 2006. Security, contingency planning, data storage, compliance, and emergency messaging are all covered in this year's program. For details on the conference go to <http://www.flaggmgmt.com/bc/>.

Continuity Forum Announces BCM Standard Briefing and Discussion

The Continuity Forum will be holding an event on February 28, 2006 in London to allow business continuity professionals to comment on the forthcoming Business Continuity Management British Standard, which is expected to be finalized this summer. The event will present the current contents of the standard to delegates and will explain its development and structure. Delegate feedback will be gathered and submitted to the BSI committee which is currently developing the standard. For more details contact sara.mckenna@continuityforum.org.

UPCOMING EVENTS

February 2006

14-16: 5th Annual Integrated Emergency Management Conference

Wellington, New Zealand

<http://www.conferenz.co.nz/2006/events/conferences/february/K034/K034.htm>

16-17: 5th Annual TISP Congress on Infrastructure Security and Homeland Security Expo

Washington, DC

www.protectinfrastructure.com

March 2006

1-2: GOVSEC Asia, Asia Law Enforcement & Asia Ready Conference & Exhibition

Hong Kong

www.govsecasia.com

7-9: First Radiological Device and Nuclear Event Symposium

Richmond, VA

Information: jroehl@scentczar.com

13-19: Business Continuity Awareness Week

UK and Europe

Information: www.thebci.org

15-16: Third Annual Business Continuity Expo

London, UK

www.businesscontinuityexpo.com

21-22: 5th Annual 2006 Business Continuity & Corporate Security Show

New York, NY

www.flagmgmt.com/bc

26-29: Disaster Recovery Journal Spring World 2006

Orlando, FL

: www.drj.com

April 2006

11-12: The 2006 Homeland & Global Security Summit

Washington, DC

www.globalsecurity.bz

May 2006

8-10: **Continuity Insights Management Conference**

New Orleans, LA

www.continuityinsights.com

23-25: **CPM 2006 WEST**

Las Vegas, NV

www.contingencyplanningexpo.com

June 2006

4-8: **National Fire Protection Association World Safety Conference and Exposition**

Orlando, FL

www.nfpa.org

18-21: **World Conference on Disaster Management**

Toronto, Canada

Information: www.wcdm.com

ROTHSTEIN ASSOCIATES INC.

4 Arapaho Rd., Brookfield, CT 06804-3104

203.740.7400 or 1.888.ROTHSTE~~in~~; fax 203.740.7401

email: Editor@rothstein.com

www.rothstein.com

Newsletter Editor: Paul F. Kirvan, FBCI

Executive Editor: Philip Jan Rothstein, FBCI

Copyright 2006, Rothstein Associates Inc. All Rights Reserved

BUSINESS SURVIVAL[™] is sent *ONLY* by YOUR subscription request!

To unsubscribe: email newsletter@rothstein.com, subject "UNSUBSCRIBE-BSN."