Volume 2 • Issue 7
July 2005

CPM™ Global Assurance

Integrating Business Continuity, Security, and Emergency Management

CONTENTS

> “Creativity is allowing yourself to make mistakes. Art is knowing which ones to keep.”
> — Scott Adams
> — the creator of Dilbert

CPM Global Assurance is a monthly subscription-based newsletter. It addresses the strategic integration of business continuity, security, emergency management, risk management, compliance and auditing to ensure continuity of operations in business and government — all within the context of good corporate governance. To subscribe to this unique resource, please fill out and fax back the subscription coupon on the back page.

See subscription coupon on last page!

PANDEMICS: Worse than CBRN Threats

By Paul Kirvan, FBCI, CBCP, CISSP

With all the focus on chemical, biological, radioactive and nuclear (CBRN) terrorist threats, CPM wants to remind its readers other threats could be just as serious – if not more serious – than CBRN events. Such a threat is an influenza pandemic. In this article, CPM examines the issues surrounding a pandemic, and in particular one focused on avian influenza.

Influenza pandemics are global outbreaks of disease that occur when a new influenza virus appears in the human population, causes serious illness, and then spreads across populations worldwide. Contrast pandemics with seasonal outbreaks or “epidemics” of influenza. Flu virus subtypes that already exist in a population typically cause epidemics. Pandemics are caused by new subtypes or by subtypes that have never circulated among people or that have not circulated among people for a long time. Previous flu pandemics have led to massive casualties, social disruption, and economic loss. The U.S. Centers for Disease Control and Prevention and the World Health Organization have large surveillance programs to monitor and detect influenza activity around the world, including possible pandemic strains of influenza virus. The World Health Organization (WHO) has developed a global influenza preparedness plan, which can be viewed at *http://www.who.int/csr/resources/publications/influenza/WHO_CDS_CSR_GIP_2005_5.pdf*.

Influenza Pandemics in the 20th Century

Last century, new influenza “A” virus subtypes caused three pandemics, all of which spread globally within a year of being detected.

- **1918-19 “Spanish flu”** [A (H1N1)] – This caused the highest number of recorded influenza deaths. More than 500,000 people died in the U.S., and up to 50 million people may have died worldwide. Influenza A (H1N1) viruses still circulate today after being introduced again into the human population in the 1970s.
- **1957-58 “Asian flu”** [A (H2N2)] – First identified in China in late February 1957, Asian flu spread to the U.S. by June 1957 and caused about 70,000 deaths here.
- **1968-69 “ Hong Kong flu”** [A (H3N2)] – First detected in Hong Kong in early 1968, it caused about 34,000 deaths in the U.S. Influenza A (H3N2) viruses still circulate today.

There is growing concern among health care agencies worldwide that the

potential for a massive influenza pandemic is increasing, and that we must be prepared for such a catastrophic event.

Dealing with Potential Flu Pandemics

Vaccines are typically used to treat influenza; however, a suitable vaccine probably would not be available in the early stages of a pandemic. The U.S. Food and Drug Administration (FDA) has approved four antiviral medications (amantadine, rimantadine, oseltamivir, and zanamivir) for treating influenza. All four counteract influenza "A" viruses. However, influenza virus strains could become resistant to one or more of these drugs, and thus the drugs may not always work. For example, the influenza A (H5N1) viruses identified in human patients in Asia in 2004 and 2005 have been resistant to amantadine and rimantadine. Monitoring of avian viruses for resistance to influenza medications continues.

How to Prepare for the Next Pandemic

Within the scientific community, the feeling is that it is only a matter of time until the next influenza pandemic. While the severity of that event cannot be predicted, modeling studies suggest that its effect in this country could be devastating. Lacking control measures (vaccination or drugs), estimates suggest that in the U.S. a "medium–level" pandemic could cause 89,000 to 207,000 deaths, between 314,000 and 734,000 hospitalizations, 18 to 42 million outpatient visits, and another 20 to 47 million people being sick. Between 15% and 35% of the U.S. population could be affected by an influenza pandemic, with an economic impact ranging between $71.3 and $166.5 billion.

Recent examples of avian influenza outbreaks and infections in Hong Kong in 1997, 1998, and 2002 and the ongoing widespread outbreaks of avian influenza among poultry in Asia, show the importance of preparing for a pandemic. It has been almost 40 years since the last pandemic.

Influenza pandemics differ from threats for which public health and healthcare systems are currently planning:

- Pandemics can last much longer than most other emergencies and may include "waves" of influenza activity separated by months.
- The numbers of healthcare workers and first responders available to work could be reduced. They are at high risk of illness through exposure in various settings, while some could miss work to care for ill family members.
- Resources in many locations could be strained considering how widespread the pandemic would be.

Because of these differences and the expected size of an influenza pandemic, planning and preparedness resources must be ready to respond promptly and adequately. The U.S. Department of Health and Human Services (HHS) supports pandemic influenza activities in the areas of surveillance ("detection"), vaccine development and production, antiviral stockpiling, research, and public health preparedness. In addition, HHS issued a draft National Pandemic Influenza Preparedness Plan in August 2004. For more details on pandemic influenza, visit the HHS Web site at *http://www.dhhs.gov/nvpo/pandemics/*.

A Big Concern – Avian Influenza (Bird Flu)

A major concern is that the next pandemic could be caused by *bird flu*, which is based on avian (bird) influenza viruses that occur naturally among birds. Bird flu viruses do not usually infect humans, but several cases of human infection with bird flu viruses have occurred since 1997.

Symptoms of bird flu in humans range from typical flu-like symptoms (fever,

Contacts

Witter Publishing
20 Commerce Street, Suite 2013
Flemington, NJ 08822
Phone 908 788-0343 • Fax 908 788-3782

Editor in Chief: PAUL KIRVAN, ext. 160
PKirvan@WitterPublishing.com

Publisher: BOB JOUDANIN, ext. 127
BJoudanin@WitterPublishing.com

Art
Art Director: MARLENE JAEGER, ext. 116
MJaeger@WitterPublishing.com

Subscriptions
Circulation Manager: BRIAN SHAPIRO, ext. 171
BShapiro@WitterPublishing.com

WPC Expositions
Director: GREGG SGROI, ext. 129
GSgroi@WitterPublishing.com

Exposition Manager: KRISTIE O'KEEFE, ext. 159
KOkeefe@WitterPublishing.com

Associate Expo Manager: COURTNEY WITTER, ext. 132
CWitter@WitterPublishing.com

Exposition Sales/List Rentals: BRAD LEWIS, ext. 154
BLewis@WitterPublishing.com

Corporate
CEO: ANDREW WITTER
Director of Finance: ANDREW SMITH
Manager, Accounting Services: LAURIE VOCKE
Director of Internet Operations: ANDY HAGG

CPM Global Assurance Newsletter (ISSN #1547-8904) is published monthly by Witter Publishing Corporation, 20 Commerce Street, Suite 2013, Flemington, NJ 08822. Subscription rates in the U.S. and Canada are $275 per year. All other countries $350 per year payable in U.S. funds.

"**POSTMASTER:** Send address changes to: Witter Publishing, 20 Commerce Street, Suite 2013, Flemington, NJ 08822"

Witter Publishing Corp. (WPC) publishes *CPM Global Assurance, Aseptic Processing & Packaging, MicroTEC,* Clean*Tech* and sponsors the CPM trade shows.
Printed in the USA

cough, sore throat and muscle aches) to eye infections, pneumonia, severe respiratory diseases (such as acute respiratory distress), and other severe and life-threatening complications. The symptoms of bird flu may depend on which virus caused the infection. Infected birds shed flu virus in their saliva, nasal secretions, and feces. Susceptible birds become infected when they have contact with contaminated excretions or surfaces that are contaminated with excretions. It is believed that most cases of bird flu infection in humans have resulted from contact with infected poultry or contaminated surfaces. Studies suggest that the prescription medicines approved for human flu viruses would work in preventing bird flu in humans. However, flu viruses can become resistant to these drugs, so they may not always work.

What Is H5N1 and Why Should We Be Concerned?

While the risk from bird flu is generally low to most people, during an outbreak of bird flu among poultry (domesticated chicken, ducks, turkeys), there is a possible risk to people who have contact with infected birds or surfaces that have been contaminated with excretions from infected birds. The current outbreak of avian influenza A (H5N1) among poultry in Asia is an example of a bird flu outbreak that has caused human infections and deaths. For more information about avian influenza issues, visit the World Health Organization website at *http://www.who.int/foodsafety/micro/avian/en/*.

Influenza A (H5N1) is subtype that occurs mainly in birds. It dates back to 1961. During 2003 and 2004 outbreaks of influenza H5N1 occurred among poultry in eight countries in Asia (Cambodia, China, Indonesia, Japan, Laos, South Korea, Thailand, and Vietnam), killing more than 100 million birds in the affected countries. By March 2004, the outbreak was supposedly under control. Beginning in late June 2004, however, new deadly outbreaks of H5N1 among poultry were reported by several countries in Asia (Cambodia, China, Indonesia, Malaysia [first-time reports], Thailand, and Vietnam). It is believed that these outbreaks are ongoing. Human infections of H5N1 have been reported in Thailand, Vietnam and Cambodia.

While the H5N1 virus does not usually infect humans, in 1997 the first case of spread from a bird to a human occurred during an outbreak of bird flu in poultry in Hong Kong. The virus caused severe respiratory illness in 18 people, 6 of whom died. Since that time, other cases of H5N1 infecting humans have appeared in Thailand, Vietnam and Cambodia. The death rate for these reported cases has been about 50 percent. Fortunately, spread of H5N1 among people has been rare and spread was usually confined to one person. However, because all influenza viruses have the ability to change, scientists are concerned that the H5N1 virus could someday infect humans, spreading easily among them. *As these viruses do not normally infect humans, very little immune protection against them exists. Assuming H5N1 could infect people and spread across populations, we could see an influenza pandemic.* While no one can predict when this might occur, experts worldwide are watching the H5N1 situation in Asia very closely and are preparing for the possibility that the virus may begin to spread more easily and widely from person to person.

How Do We Deal With H5N1?

The H5N1 virus is resistant to amantadine and rimantadine, but two other medications, oseltamivir and zanamivir, might work. However, studies are needed to prove that they work. There currently is no vaccine to protect humans against the H5N1 virus in Asia. However, vaccine development efforts are under way. Research studies to test a vaccine to protect humans against H5N1 virus began in April 2005. Work is also being done on a vaccine against H9N2, another bird flu virus subtype. For more information about the H5N1 vaccine development process, visit *http://www2.niaid.nih.gov/Newsroom/Releases/flucontracts.htm*.

How is CDC Preparing for an H5N1 Pandemic?

CDC is involved in several pandemic prevention and preparedness activities, including:

- Working with the Association of Public Health Laboratories on training workshops for state laboratories on the use of special laboratory (molecular) techniques to identify H5 viruses;
- Working with the Council of State and Territorial Epidemiologists and others to help states with their pandemic planning efforts;
- Working with other agencies such as the Department of Defense and the Veterans Administration on antiviral stockpile issues;
- Working with the World Health Organization (WHO) and Vietnamese Ministry of Health to investigate H5N1 in Vietnam and to assist in laboratory diagnostics and training to local authorities;
- Performing laboratory testing of H5N1 viruses;
- Starting a $5.5 million initiative to improve influenza surveillance in Asia;
- Involvement in training sessions to improve local capacities to conduct surveillance for possible human cases of H5N1 and to detect influenza A H5 viruses via laboratory techniques;
- Developing and distributing reagents kits to detect existing influenza A H5N1 viruses; and
- Collaborating with WHO and the National Institutes of Health (NIH) on safety testing of vaccine seed candidates and to develop additional vaccine virus seed candidates for influenza A (H5N1) and other subtypes of influenza A viruses.

Conclusion

At the moment, the risk to Americans from the Asian H5N1 outbreak is low. The Asian strain of H5N1 has not been observed in the U.S. However, it is possible that travelers returning from affected Asian countries could be infected. Since February 2004, medical and public health personnel have been watching closely to find any such cases. CPM encourages continued vigilance, research, and preparedness. ■

CNT Shareholders Approve Acquisition by McDATA

CNT (Minneapolis, MN), a provider of storage networking solutions, recently announced that its shareholders have approved McDATA Corporation's proposed acquisition of CNT. *www.cnt.com*

VeriSign Receives DOD Certification (Federal Computer Week)

VeriSign (Mountain View, CA) has recently been accredited by the U.S. Department of Defense to expand its digital certificate services to federal, state and local governments. The certification, which VeriSign obtained under DOD's External Certificate Authority (ECA) program, also authorizes the company to issue digital certificates to individual employees of state and local governments, businesses and foreign governments. Digital certificates provide an additional layer of security for e-mail and remote Web site access by authenticating users' identities online. People also use them to digitally sign documents and electronic forms. *www.verisign.com*

ESS Partners with AudienceCentral

ESS (Tempe, AZ), a provider of environmental, health and safety (EH&S) and crisis management solutions, and AudienceCentral (Bellingham, VA), a provider of communications software, announced a partnership agreement today that is expected to help clients reduce information response times during unexpected or unforeseen events. The primary tools are AudienceCentral's Public Information and Emergency Response (PIER) system, which provides users with one central web-based platform for drafting, approving, and distributing up-to-the-minute content to all target audiences and stakeholders, and Essential Incident Master™ by ESS. Essential Incident Master software meets all requirements of the National Incident Management Systems (NIMS) and Incident Command System (ICS), while continuing to address daily and emergency response operations. *www.ess-home.com*; *www.audiencecentral.com*.

New CEO Joins Whale Communications

Whale Communications (Fort Lee, NJ), a provider of SSL (secure socket layer) VPN solutions, recently announced the appointment of industry veteran Roger J. Pilc to Chief Executive Officer. The company also announced that it secured $6.5 million in additional funding led by existing investors Goldman Sachs, Soros Fund Management LLC and the BRM Group. Pilc replaces co-founder and CEO Elad Baron who will remain on Whale's Board of Directors.

U.S. to Compromise on Biometric Passports

In a policy shift designed to avoid serious transatlantic travel disruptions, the U.S. is positioning itself to drop its demand that European nations and other close allies adopt biometric passports by October 2005, according to U.S. and European government officials. However, the compromise could strain relations by differentiating among European countries, and in particular by requiring some French and Italian citizens to obtain visas before they travel to the U.S. For more than two years Washington has insisted, based on security reasons, that countries whose citizens can enter the U.S. without visas begin issuing biometric documents that ensure the identity of the passport holder. The plan is the latest in a series of twists since Congress passed legislation in 2002 that required the 27 countries in the so-called visa-waiver program to start issuing the high-tech passports by October of last year. Brussels has said that some European countries in the program will not be able to meet that requirement until August 2006.

ACP Announces Cleveland, OH Chapter

The Association of Contingency Planners (ACP), a leading organization for business continuity professionals, has chartered its first chapter in the state of Ohio. Located in Cleveland, OH the "Northern Ohio" chapter will provide networking, educational, and professional development services. Brian Zawada is chapter president. Contact at *brian.zawada@protiviti.com*. *www.acp-international.com*

BNET Announces Stamford, CT Joins CEAS Family

Dr. Robert H. Leviton, President of the Business Network of Emergency Resources, Inc (BNet), recently announced the City of Stamford, CT as the newest member in the growing family of governments using the Corporate Emergency Access System (CEAS) to assist business recovery following a serious emergency or disaster. Stamford joins New York City, Boston and Buffalo in using the CEAS program.

CEAS is a public/private partnership that permits designated individuals from local businesses to re-enter areas restricted to public access due to emergency conditions. *www.bnetinc.org*; *www.ceas.com*

Network Security Market Up 5% in 1Q05

Worldwide network security appliance and software revenue was up 5% between the last quarter of 2004 and the first quarter of 2005, and is forecast to grow 27% to $1.3 billion in the first quarter of 2006, according to Infonetics Research's (San Jose, CA) quarterly worldwide market share and forecast service, *Network Security Appliances and Software*. Total annual revenue is expected to grow to $6.5 billion by 2008. For the table of contents, go to *www.info.infonetics.com*

FEMA Announces Two New Web-Based Incident Command System (ICS) Courses

Michael D. Brown, Under Secretary of the U.S. Department of Homeland Security (Emmitsburg, MD) for Emergency Preparedness and Response, recently announced that the nation's first responders can now take two new Incident Command System (ICS) courses online through the Federal Emergency Management Agency (FEMA) Virtual Campus. The two courses were jointly developed by FEMA's U.S. Fire Administration and the U.S. Department of Agriculture's National Wildfire Coordinating Group (NWCG).
Now available are:

Q-462 - *Introduction to All-Hazards NIMS ICS for Operational First Responders* and

Q-463 - *Basic All-Hazards NIMS ICS for Operational First Responders*

For details go to *http://training.fema.gov/* and click on Online Training (NETCVirtual Campus).

Report: 36 Percent of World's Archived Data Stored on StorageTek Equipment

StorageTek (Louisville, CO), a provider of data storage solutions, has been recognized in a report from analyst firm Freeman Reports. The report, "The Growing Importance of Archive," found that StorageTek led the industry with 36 percent of the world's total archived data, followed by IBM with 16 percent, ADIC with 15 percent, Overland with 10 percent and Quantum with nine percent.
www.storagetek.com ■

International News

■ *www.continuitycentral.com*

BridgeHead Facilitates Data Backup and Restoration for Galway Clinic

Galway Clinic (Galway, Ireland), a new hospital in western Ireland, selected BridgeHead Software's (Woburn, MA) HT Backup technology to provide automated backup and restoration for its central healthcare information system (HCIS) and picture archiving and communications system (PACS). Galway Clinic uses the latest technology to facilitate how it delivers healthcare. By removing the reliance on paper-based records, its IT system allows doctors and nurses instant access to patient information and digital images at the touch of a button from anywhere in the hospital. BridgeHead's HT Backup talks through an API with the Meditech HCIS application, to provide image based backup of the application data. A unique feature of BridgeHead's software is that the backup process works without relying on the CPU resources from the application server, so there is no slowing down in performance of the central health informatics system and users can continue to access data at all times. *www.GalwayClinic.com*
www.BridgeHeadSoftware.com

Dubai's Day Without Power (Source: Gulf Times)

A major blackout on June 9 resulted in business continuity problems for Dubai-based firms. At 9.47am local time all power and telecommunications supplies in the emirate were lost, with full restoration not complete until 5.00pm the same day. Costs of the blackout were estimated at Dh11m an hour. Mohammed Amin, regional manager, EMC Middle East, told Gulf Times, "Today's power outage in Dubai vividly highlights the need for firms in every sector including telecommunications, banking, energy and government to have in place a viable business continuity strategy that is regularly tested for occasions such as these." This is the second time such an event took place in four years. In 2001, a failure in a power station in Jebel Ali disrupted electricity and the water supply in the city.

BCI Launches Pakistan Business Continuity Forum

Ghazali Wasti, the Business Continuity Institute's (Reading, UK) regional representative for Pakistan, has announced the formation of Continuity Pakistan, the BCI's latest regional business continuity forum. The forum's aims are to raise awareness of business continuity in the region, communicate and participate with Pakistan's government and financial sector to develop a good practice guide to business continuity, initiate regional business continuity conferences, and deliver introductory seminars offering basic information about business continuity planning. Continuity Pakistan has nominated a Central Executive Committee to help develop the forum.
For further details contact *gawasti@yahoo.com; www.thebci.org*

New Earthquake Warning for Sumatra Region

The second earthquake in South Asia in three months increased stress on fault lines in the region, making it vulnerable to another rupture and a tsunami, according to recent comments by scientists. "We're concerned about a large earthquake and there is a strong probability that if it happens, it will generate a tsunami," Professor John McCloskey of the University of Ulster told Reuters. He and his team, who predicted the March 28 quake about two weeks before it occurred, said the area under the Mentawai islands west of Sumatra is most at risk of an earthquake with a magnitude of 8-8.5 or stronger.

Tsunami Could Strike Australia in Next Decade

Australia's populous east coast could be struck by a devastating tsunami during the next decade, researchers said recently as the government prepares to create a national tsunami warning system. Australia is surrounded by 8,000 km (5,000 miles) of active tectonic plate boundaries capable of generating tsunamis that researchers and the government say could reach the country's coastline within two to four hours. One third of the world's earthquakes take place along these boundaries, they said. Professor Peter Mora, director of the Earth Systems Science Computational Centre at the University of Queensland, said there was a misconception Australia was safe from earthquakes and tsunamis, when the country was instead very prone. "Our international research collaboration partners in the USA forecast that within the next 10 years, a great earthquake with a magnitude of at least 7 on the Richter scale is likely to strike to the north of New Zealand," Mora said. "This could mean a potential tsunami hazard for the east coast of Australia." New Zealand would also be hit hard and possibly low-lying Pacific island states to the north. New Zealand, about 2,000 km east of Australia, straddles two of the tectonic plates that make up the Pacific "ring of fire". Geoscience Australia is setting up Australia's A$70 million ($53 million) tsunami warning system. (US$1 = A$1.32)

Increased Reliance on IT Driving BC Purchases

A recent UK survey by SunGard Availability Services (London, UK) has found that the majority of respondents (52 percent) cited an increased reliance on IT as the main driver behind their firm's business continuity strategies. This contrasts with the results of 2003 survey, where the threat of terrorism was seen as the main driver (34 percent of respondents said that this was the top factor driving business continuity investment). Two years ago, an increased reliance on IT was the main driver for only a quarter of firms surveyed. The 2005 survey found that new regulations were the second highest factor encouraging increased investment in business continuity, with 33 percent of respondents saying that this was their top reason for making business continuity purchases. *www.sungard.co.uk*

Permanent Deep-Sea Sensors Set Up to Monitor Seismic Activities

Europe's first permanent deep-sea seismic sensor will help to provide early warning of tsunamis. A submarine seismic sensor was recently set in place at a depth of 2,400m, off the French coast near Toulon. The instrument was attached to a neutrino telescope developed by the international scientific programme Antares. For the first time in Europe, this sensor, designed by a partnership between Géosciences Azur (Mixed Research Unit IRD/CNRS/UPMC/UNSA, Villefranche sur Mer) and Guralp System (United Kingdom), with the financial support of INSU, Villefranche Oceanological Observatory and the Provence-Alpes-Côte d'Azur Regional Council, can send real-time deep-sea seismic activity data recorded for the region and for the whole world. Until now sensors have been dropped from the sea surface and allowed to drift to the ocean floor. These devices record several months' seismic activity and are retrieved for data analysis. The new permanent sensor uses a 40km long cable which links all the elements of the Antares experiment to the coast; from where data is relayed via the Internet to the Géosciences Azur laboratory. ■

GLOBAL ASSURANCE PRODUCTS

MIR3 Announces inGovAlert for Emergency/First Responder Communications

MIR3 (San Diego, CA), a provider of emergency notification solutions, recently unveiled inGovAlert. It provides government organizations, including first responders and homeland security agencies, with a GSA-authorized solution for emergency communications using MIR3's Intelligent Notification technology. The product supports intra-agency communications and cooperation in the event of a disaster, emergency or severe weather crisis. It facilitates sending of high-speed emergency communications to and from any device, such as landline, satellite and mobile phones, email, pagers, SMS, PDAs and fax, to individual recipients, groups or organizations with the click of a button. inGovAlert is available now as a hosted or on-premise solution and can be purchased via the GSA schedule. *www.mir3.com*

Ontrack Data Recovery Launches VeriFile

Ontrack Data Recovery (Minneapolis, MN) has introduced Ontrack® VeriFile™ Online Data Reports that let customers view a complete listing of their recoverable and non-recoverable files in an organized, easily searchable format. By means of a small browser-based application, the new VeriFile reports offer customers the ability to make a more informed decision about their data recovery. For an average investment of $100, Ontrack

GLOBAL ASSURANCE PRODUCTS

VeriFile provides an easy-to-read report format that provides the customer with details related to the initial assessment of the data loss, quickly identifying for the customer the quality of the recovery available. VeriFile is compatible with Microsoft Internet Explorer 5.x or greater and is available for most data recovery evaluations. For more information about VeriFile, visit *www.ontrack.com/verifile/compare.asp*, *www.ontrack.com*

eSafe 5 Powers Enterprise Spyware Protection

Aladdin Knowledge Systems, Inc. (Chicago, IL), a provider of digital rights management software and content security and authentication solutions, has announced Aladdin eSafe 5. The product provides web security in large organizations by addressing spyware/adware threats with multi-layered comprehensive content protection. Also introduced in Aladdin eSafe 5 is a gateway solution featuring four layers of spyware protection. Featuring 17 spam-blocking technologies, Aladdin eSafe offers spam tagging, blocking, remote quarantine and user-managed quarantine and reports. *http://www.Aladdin.com/eSafe5.*

NSI Software Enhances Double-Take

NSI Software, Inc. (Hoboken, NJ), developer of Double-Take®, a solution for continuous data protection and application availability, recently announced enhancements to Double-Take®, including the introduction of EnterpriseView Server Groups. This feature lets system administrators quickly organize, monitor, and manage hundreds of Double-Take® servers across enterprises at a single glance. The management console looks much like Windows Explorer, and groups servers in a logical hierarchy. NSI expanded existing Double-Take® features with Enhanced Failover Monitor and Target Reboot Without a Mirror capabilities. The company has also launched specialized Enterprise Disaster Recovery (E-DR) workshops through its professional services organization. *www.nsisoftware.com*

Announcements from Lakeview Technology

Lakeview Technology (Oak Brook, IL), a provider of infrastructure software, recently announced more extensive self-healing, continuous assessment, deeper audits and ease-of-use features in its MIMIX® ha1™ and MIMIX® ha Lite™ high availability (HA) solutions. The new features improve the total health and quality of HA environments. The new autonomics and ease of use features are free to customers with a current MIMIX® hA maintenance agreement. The company also announced participation in an IBM program in which free evaluation versions of Lakeview's MIMIX® dr1™ availability software will be distributed with all IBM® i5/OS™ (OS/400 V5R3) installation disks bundled with new iSeries servers and upgrade packages. MIMIX dr1 is a low-cost enhanced recovery solution that lets users capture recovery points periodically throughout the day - dramatically reducing exposure for data loss in the event of a disaster. *www.lakeviewtech.com*

Red Earth Software Releases Policy Patrol Web for Microsoft ISA Server

Red Earth Software (Portsmouth, NH), developer of content security software, recently unveiled Policy Patrol Web 1.0 for Microsoft's Internet Security and Acceleration (ISA) Server. By allowing companies to create flexible, user-based content filtering rules, Policy Patrol Web helps companies manage their Internet resources according to each of their user's needs. Policy Patrol Web integrates closely with ISA Server 2000 and 2004 and performs URL checking, keyword filtering, file checking, virus and spyware blocking and real-time monitoring.
A 30-day evaluation version is available from *http://www.policypatrol.com*; *http://www.redearthsoftware.com*

Amacom Unveils Backup Software

Amacom Technologies U.S. Ltd (Atherton, CA), developers of portable, high capacity data storage devices, have announced Flipback Version 3.0™. An enhancement to the Flip2disk™ product family, Flipback V3 features increased functionality and time saving featureslike selective synchronization, which result in the backup process now taking a few minutes rather than hours to run, and the ability to profile automatic backups. *www.amacomus.com*

Announcing ERBUS

Over the past decade, the world has witnessed a multitude of natural disasters and tragedies. Millions suffered because aid and basic needs were not received in an adequate amount of time. A humanitarian technology called ERBUS, Emergency Response Backup Utility System, has been developed to respond to emergency situations by providing critical resources necessary for survival including portable purified water, electric power, filtered air, and communications. Invented by Deborah Yungner, ERBUS can also serve as a sheltered enclosure, clinic, counseling center, or shower facility. The unit is designed to be positioned in any disaster are and can be transported via air, land, or water. *www.erbus.us*

MGE Unveils New Power over Ethernet (POE) Solution

MGE UPS Systems, Inc. (Costa Mesa, CA), a provider of power protection solutions, has announced the launch

GLOBAL ASSURANCE PRODUCTS

of its new Power over Ethernet (PoE) midspan products (also known as power hubs). The new devices ensure continuous power to remotely connected IP telephones, wireless LANs, Bluetooth access points and IP-powered video surveillance and security systems, when used in conjunction with an MGE uninterruptible power supply (UPS). PoE integrates power and data onto a single CAT 5/5e and 6 cabling infrastructure, eliminating the need to install separate electrical wiring and power outlets. MGE's midspan units feature a two-year warranty and meets UL/cUL, CE, FCC Part 15, Class B with FTP cable standards and approvals. Available now, the midspan unit costs $1,199; the SNMP version lists for $1,499.
www.mgeups.com

New Identity Verification Report Helps Employers Detect Fraud

Employment screening firm OPENonline LLC (Columbus, OH), recently announced its online National Identity Verification Report that gives employers a quick and cost-effective tool to learn if applicants are presenting their true identities. The OPENonline Identity Verification Report determines if an applicant's reported social security number was in fact issued by the Social Security Administration and, if so, when and where it was issued. The report also provides the name and related address history of anyone using or linked to that social security number as well as reporting if the number has been associated with a death benefit claim.
www.openonline.com

Case Study – How Jacksonville Uses Technology to Survive Hurricanes

As we progress through the 2005 hurricane season, many lessons can be learned from cities in Florida. In this article, CPM interviews Dave Lauer, CIO for the City of Jacksonville, FL, on how the city has responded to hurricanes using advanced technology.

Located in Northeast Florida at the crossroads of two interstate highways, Jacksonville is the 14th largest city in the U.S., with a metro area population of over one million. The city is the insurance and financial center of the state, the site of U.S. Navy bases, and hosted Super Bowl XXXIX earlier this year. The city's Information Technologies Division handles all areas of technology for the city, and has an annual operating budget of approximately $40 million.

CPM – What previous experience - negative or positive - did the City of Jacksonville have with hurricanes that affected its IT operations, specifically access to the IT infrastructure?

Dave Lauer – Jacksonville had not experienced a hurricane as severe as Frances, which struck in September 2004, in about 40 years. We had a large number of downed trees and a great deal of debris, which caused a lot of power outages. For some people, power was out for less than a day, but some people in more remote areas did not have power for several weeks.

CPM – What happened as a result, and how did the city respond/cope with the situation?

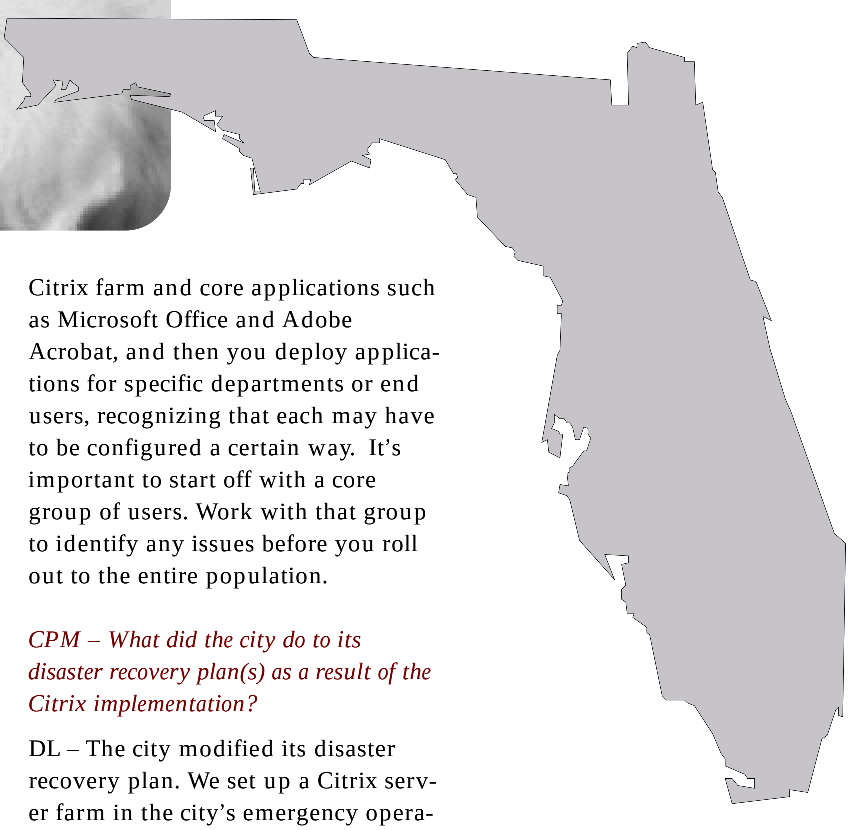
DL – Jacksonville Electric Authority (JEA), the city's electric and water utility, got flooded with phone calls. We (the Information Technologies Division) stepped in to assist, covering additional calls. We even partnered with a local vendor to use its call center facilities for overflow. By providing that overflow capability, we were able to handle literally thousands of calls in a short period of time. Folks were able to get through and speak with real people. City employees who decided to evacuate were still able to access city services via our Citrix access infrastructure. With Citrix we were able to provide connectivity to applications in the field and remotely. Cleanup crews, for example, could update their database in real time so city officials knew which areas still needed help.

CPM – How did the city determine where its infrastructure was at risk, based on the impact of prior hurricanes?

DL – Primarily, the power grid was impacted. JEA learned a great deal from Frances, and has devised a number of contingency plans. One of the major areas was communication. You always have some capability, but we received thousands of calls in a very short period of time. For this year's hurricane season, we devised plans for setting up temporary call centers on the fly, so that we're able to reroute calls within minutes or seconds. Where there is debris, we can plot it on the city's geographic information system (GIS), so we know the major areas that are affected.

CPM – What process did the city use to source their solution, and why did officials select that particular product?

DL – It was coincidental that we were rolling out Citrix Access Suite as hurricane season was upon us. I have



used Citrix for a number of years. We were looking at it for improving government efficiency, extending the life of systems, and providing remote access for folks outside the office or for mobile workers. We procured it using a General Services Administration pricing model, and we worked with Citrix to ensure we got the best pricing.

CPM – What did the city do to its infrastructure so that Citrix could be successfully deployed?

DL – As part of a typical Citrix implementation, we built up a Citrix server farm and spent time with Citrix to ensure we had all the elements appropriately configured. We went through a pilot phase to ensure we worked out any issues ahead of time. That required an investment on our part in time and in the core infrastructure (server farm). To provide access in the field, we selected Verizon's EVDO (Evolution Data Optimized) wireless broadband Internet access for remote connectivity. With Citrix and EVDO, we can provide any application anywhere, at any time.

CPM – What lessons did Jacksonville learn about a Citrix deployment?

DL – I've handled several Citrix implementations in previous jobs, and we were able to apply those lessons. One of the lessons is to ensure you have a solid foundation, design and architect effectively, and spend time working out any end-user issues before going into production. When publishing applications over Citrix, you must ensure they are appropriately configured in the Citrix environment. You begin by setting up your Citrix farm and core applications such as Microsoft Office and Adobe Acrobat, and then you deploy applications for specific departments or end users, recognizing that each may have to be configured a certain way. It's important to start off with a core group of users. Work with that group to identify any issues before you roll out to the entire population.

CPM – What did the city do to its disaster recovery plan(s) as a result of the Citrix implementation?

DL – The city modified its disaster recovery plan. We set up a Citrix server farm in the city's emergency operations center to run core applications. If our main data center went down, production would move to the emergency operations center. That would happen almost immediately if we lost the data center. Service for emergency or critical users would not be interrupted.

CPM – What happened as a result of the Citrix system being in place during Hurricane Frances that was different from the city's previous experience?

DL – Any city employee could stay connected outside the office, and field workers could access applications in real time. As a result, city services could continue in the event of an emergency.

CPM – What are the city's next steps toward ensuring uninterrupted IT operations, now that hurricane season is officially underway?

DL – For this season, we have a comprehensive plan in place for redundant telecommunications. We have plans for interoperability with the city, the school system and the electric utility to make sure we are leveraging each other's infrastructure. The secondary Citrix farm will kick in if the main Citrix farm goes down for any reason. We are increasing our use of GIS in the field to prioritize service calls and update their progress in real time. We map the problem, address it, and report it so city officials can look at a real-time map and do real-time planning in the event of an emergency. ■

About the Author

Dave Lauer is Chief Information Officer for the City of Jacksonville, Florida, where he is responsible for identifying technology solutions to improve service to the citizens of Jacksonville, increase efficiency, and lower costs. Lauer has over 15 years of information technology experience.

Lists – We Have Lists

CPM receives all kinds of information each month. As such, we've been accumulating a number of interesting lists and we'd like to share them with you over the next few pages.

Top 10 Hurricanes and Estimated Insured Losses (Adjusted to 2004 Dollars)

From ISO's Property Claim Database

Year	Event	Insured Loss
1992	Andrew	$20.8 billion
2004	Charley	$7.5 billion
2004	Ivan	$7.1 billion
1989	Hugo	$6.4 billion
2004	Frances	$4.6 billion
2004	Jeanne	$3.7 billion
1998	Georges	$3.4 billion
1965	Betsy	$3.1 billion
1995	Opal	$2.6 billion
1999	Floyd	$2.2 billion

Source: *www.iso.com*

Top Five Ways State/Local Government Officials Can Prepare for a Hurricane

By Keenan Baker, CDW Government, as identified in the *CDW Business Continuity Guide*

1. Back up data frequently to ensure daily records are kept, and consider upgrading the backup equipment to a higher-speed version to reduce the time it takes to complete a backup cycle;

2. Add uninterrupted power supplies for critical servers, network connections, and selected PCs to keep the most essential applications running;

3. Arrange for data replication to a second, remote server outside of the area threatened by the hurricane, in case of an emergency at the original site housing the data;

4. Create lists of emergency contacts and instructions; distribute them to all appropriate government workers; and

5. Form tight relationships with hardware and service vendors, who can often ensure priority replacement of telecommunications equipment, personal computers, servers, and network hardware in a disaster.

Source: *www.cdwg.com*

Five Steps to Ensure Effective Emergency Communications

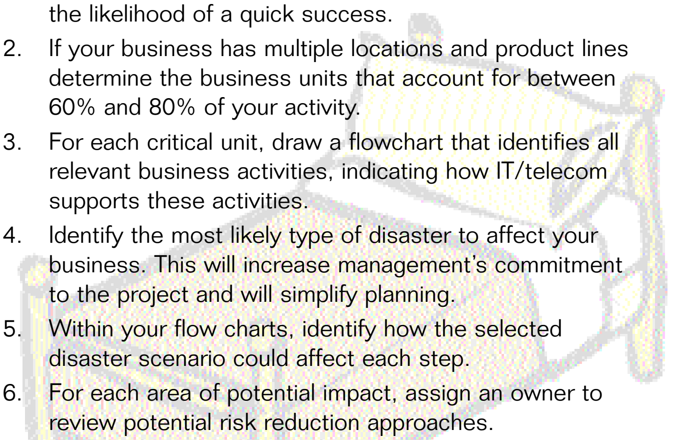
By EnvoyWorldWide

1. Never rely on a singular mode of getting emergency messages out; couple voice messages with email, SMS, fax, Blackberry, etc.
2. Use clear language and headers in your notification to avoid filters.
3. Make sure your messaging service provider has relationships with multiple ISPs and their white lists to avoid being labeled as spam.
4. Make sure your notification system escalates seamlessly among device types, based on predefined parameters.
5. Test, test, test – make sure emergency notification systems work properly

Source: *www.envoyworldwide.com*

Ten Steps to Help CFOs Sleep Better

By John Schaefer



1. Divide your business into manageable units to increase the likelihood of a quick success.
2. If your business has multiple locations and product lines determine the business units that account for between 60% and 80% of your activity.
3. For each critical unit, draw a flowchart that identifies all relevant business activities, indicating how IT/telecom supports these activities.
4. Identify the most likely type of disaster to affect your business. This will increase management's commitment to the project and will simplify planning.
5. Within your flow charts, identify how the selected disaster scenario could affect each step.
6. For each area of potential impact, assign an owner to review potential risk reduction approaches.
7. For each area on the flowchart where IT support is identified, provide detail on primary and secondary systems, plus a simple "high-medium-low" priority rating for each.
8. For each critical system, assess the impact of 1) inappropriate access by employees or outsiders, 2) damage to the integrity of the information, and 3) lack of availability.
9. Assign a coordinator for overall IT security reviews whose job is to collect information about exposures and to facilitate discussions on how priorities can be agreed.
10. Select no more than ten critical risk reductions to be completed during the quarter. Assign tasks, deadlines and resources to specified individuals. Monitor this quarterly.

About the Author

John Schaefer is Vice President, Enterprise Risk Management, with ABD Insurance and Financial Services, based in Redwood City, CA. *www.abdi.com*

Six Ways To Protect Against Zero-Day Attacks

By Rob McCarthy

Recently, damage from a series of viruses and worms – the MS Blaster, Slammer, Sasser, and Korgo W worms – has shown how vulnerable computer systems are. Signature-based anti-virus software and traditional firewalls are not enough to protect networks. There are growing concerns about *zero-day attacks*, based on previously unknown vulnerabilities and completely immune to anti-virus software. Here are six ways to protect your networks.

1. Use file integrity checking – This process informs you if the software you think you have installed on your network is actually what it is supposed to be. Tripwire is a free utility that can check this. File integrity checking is also useful for discovering spyware and viruses your anti-virus software has missed.

2. Run new or unknown software in a sandbox – New anti-virus software extends file integrity checking by making unknown software run in an isolated capacity, called a "sandbox." This technique prevents viruses or worms from propagating unless they can trick a known program into doing the work for them. One way to develop a sandbox is to use Microsoft's Active Directory to keep users from installing anything new. The network administrator must check new software before it is installed.

3. Scan autoruns – PC autorun programs should be periodically scanned for threats, as they are a favorite entry point for viruses, worms, and spyware. A utility called Autoruns from SysInternals will scan everything being run when you boot up your PC.

4. Use intrusion prevention at gateways and on desktops – Intrusion prevention software normally monitors network traffic and matches it against known types of attacks. Vendors continually update intrusion prevention rules.

5. Use heuristic and signature-based anti-virus software – While most networks use this software, recent offerings help users create their own virus signatures and to distribute them throughout their networks.

6. Be aware of Microsoft holes – While Microsoft systems and programs are known for their vulnerabilities, some software vendors have extended Microsoft's security by adding *program permissions* to Windows. Just as users have permissions for directories and files, programs can have permissions to access different parts of the operating system, giving direct control over what can and cannot be done.

About the Author

Rob McCarthy is president of network security firm Lightspeed Systems. *www.lightspeedsystems.com*
Source: *www.networkingpipeline.com*

Eight Top Tips to Ensure Network Security

From the Networking Pipeline

1. **Define policies and ensure governance –** With new regulations like Sarbanes-Oxley raising the bar for corporate responsibility, governance has become particularly critical. Policies need to be very explicit.
2. **Educate users –** The rules themselves are useless if no one knows what they are. To protect networks on the outside it's essential that users on the inside know what they can and cannot do safely.
3. **Put someone in charge –** It's not just an IT function any more. Protecting networks is a full-time job, and someone in the firm must be responsible for it.
4. **Configure your hardware –** Despite the abundance of plug-and-play products, there's no guarantee that the products will work correctly, unless you get involved. Even basic network hardware and software not directly related to security must be properly installed and configured.
5. **Keep an eye on remote users and portable devices –** This is a key entry point for unauthorized malware. For example, even though the network perimeter is secure, users who log into unprotected wireless networks other than the office can find themselves transporting malware into the company.
6. **Protect your e-mail –** Unencrypted e-mail makes it easy for people to read your messages. Ironically, e-mail is the most vulnerable network application because it is the most ubiquitous and trusted application. Encryption is essential.
7. **Embrace diversity –** Variations in network composition, despite vendor advice to establish homogeneous environments, are a good thing. Homogeneous networks are usually easier to crack, whereas heterogeneous solutions are harder to compromise.
8. **Lock down the physical premises –** Despite the convenience of on-line and remote computing, don't forget to secure the building and the network infrastructure. Better the inconvenience of a locked door than the loss of thousands of dollars of valuable equipment or data.

Source: *www.networkingpipeline.com*

Identity Crisis: Who Are We, and What Are We Doing?

By Gregg Jacobsen

"Whooooo are you? Doot-dooo-doot-doot! I really wanna know…" This lyric, written by The Who in the 1960s, is a relevant question for those of us who help clients and employers determine what to do when calamity strikes. Gregg Jacobsen takes a look at a major conundrum of the BC profession.

So what DO we as contingency planning professionals really do? Consider our titles: business continuity planner, disaster recovery planner, emergency operations manager, DR analyst, BC coordinator, operational continuity consultant, IT continuity planner, and so on. This is only a sampling of the job postings among the various recruiting websites, but the common thread is that we are people who spend our time trying to think of ever better ways to prepare for disastrous events. We do risk assessments, operational impact and gap analyses. We develop preventive and mitigation strategies and plans to implement them. We test the plans and work to improve their effectiveness, all because something bad may happen. The common thread is that "something," and it has a name: *contingency.*

What's a Contingency?

Simply put, it is a potential event, something that *could* happen. Fires, floods, hurricanes, tornadoes, tsunamis, earthquakes, labor actions, civil unrest, product tampering, and workplace violence are all contingencies. When a business or government agency wants to prepare for unplanned emergencies, they want a contingency planning professional. That's us.

So What's the Crisis?

The problem with this identity crisis is that many of our fellow professionals are toiling away in anonymity; misplaced in the food chain of the industries they serve. Consider the business continuity planner, chartered to bulletproof critical operations of his/her employer by strategizing manual work-arounds, work area recovery solutions and the like. In nine out of ten corporations, according to industry surveys, this position is buried within IT departments, where even the bosses don't "get" business continuity. To them, BC equals DR – disaster recovery, the resurrection of the IT infrastructure.

You Beg to Differ?

For those who think this is a distorted view, please visit Internet websites that post job openings. You will find, as has this writer, that nearly all BCP "recruiters" work for IT staffing firms with clients that have a BCP opening in the IT department. The problem with being associated with IT is that the market for IT talent has seen a severe drought in the last few years, with salaries and contract hourly rates plummeting. And the price for BCP talent went with them because that's where they've been positioned.

Overhead: the Greatest of Evils

Among the greatest of evils facing contingency planners is overhead: the recurring costs for having a place of business, lighting and heating, and of course an IT infrastructure. So, IT costs are overhead, and contingency planners have sadly been lumped in with IT staff. The IT services industry has even co-opted "business continuity planning" for its own use, primarily to sell consulting clients on the idea they actually DO such work. Were that true, they might hire people with at least a basic understanding of business operations, and how to plan for their continuance or resumption after an unplanned interruption. The problem for us has become one of visibility. Those of us who practice contingency planning have become lost in the IT crowd, and IT recruiters and employers simply can't see us.

Long May It Wave

So, let's re-identify our profession in a way that distinguishes us from the IT community:

- Let's start using "Contingency Planning Professional" on our business cards.
- To people who ask, "What do you do for a living?" let "contingency planning" be your answer.
- Get involved with others who share our common interest in contingency planning.

A good option is to join up with professional groups such as the Association of Contingency Planners in the U.S., the Disaster Recovery Information Exchange in Canada, and Survive in Europe. By affiliating with such groups, we can forge a clear identity as members of a recognized profession. Let us resolve to join such groups and raise our own new banner: "Contingency Planners Unite!" Well, maybe we'll have to come up with a different phrase – "CPU" is, after all, an IT term. ■

About the Author

Gregg Jacobsen, CBCP, is a contingency planning consultant with over eight years experience working for public agencies and private sector industries. He is president of the Association of Contingency Planners Los Angeles Chapter and Chairman of the ACP Presidents' Council.

EVENTS CALENDAR

July 2005

10-13: **World Conference on Disaster Management**
Toronto, Canada
Web: www.wcdm.org

10-13: **International Symposium on Risk Management and Cyber-Informatics**
Orlando, FL
Web: www.cyberinformatics.org/rmci05/

11: **Capitol Hill BioDefense Showcase**
Washington, DC
Web: www.globalsecurity.bz

12-13: **Emergency Preparedness for Government Facilities**
Colorado Springs, CO
Web: www.homelanddefensejournal.com;
Email: pgreenstein@marketaccess.org

18-22: **Business Continuity Training Seminar**
Toronto, Canada
Web: www.sentryx.com

21-22: **Strategy to Reality Seminar, IP3**
San Francisco, CA
Web: www.ip3seminars.com/u/rcs51016.php

27-28: **Black Hat Briefings 2005**
Las Vegas, NV
Web: http://www.blackhat.com/html/bh-usa-05/bh-usa-05-schedule.html

29-31: **Defcon 13**
Las Vegas, NV
Web: http://www.defcon.org/html/defcon-13/dc13-index.html

August 2005

1-2: **Securing VoIP and Wireless Communications**
Chicago, IL
Web: http://www.voip-wifi.net/u/rcs51001.php

8-11: **InfraGard 2005 National Conference**
Washington, DC
Web: www.infragardconferences.com

September 2005

12: **EurOhse2005 One-day Masterclass on Fire Risk Assessment and Business Continuity Planning**
London, UK
Web: www.eurohse2005.com

12-14: **Information Lifecycle Management (ILM) Summit**
East Rutherford, NJ
Web: www.ilmsummit.com

12-15: **51st Annual ASIS International Seminar and Exhibits**
Orlando, FL
Web: www.asisonline.org

13-14: **Strategy to Reality Seminar, IP3**
Austin/Houston, TX
Web: www.ip3seminars.com/u/rcs51016.php

20-21: **U.S. Maritime Security Expo**
New York, NY
Web: www.maritimesecurityexpo.com

20-21: **Strategy to Reality Seminar, IP3**
Detroit, MI
Web: www.ip3seminars.com/u/rcs51016.php

27-28: **Strategy to Reality Seminar, IP3**
Seattle, WA
Web: www.ip3seminars.com/u/rcs51016.php

28-30: **IT Security World 2005**
San Francisco, CA
Web: www.misti.com

October 2005

18-19: **Strategy to Reality Seminar, IP3**
Washington, DC
Web: www.ip3seminars.com/u/rcs51016.php

25-26: **SIA Business Continuity Planning Conference & Expo**
Brooklyn, NY
Web: www.sia.com/bcp05/

25-26: **Strategy to Reality Seminar, IP3**
Phoenix, AZ
Web: www.ip3seminars.com/u/rcs51016.php

31-Nov 2: **7th Annual Technologies for Critical Incident Preparedness Conference and Exposition 2005**
San Diego, CA
Web: www.ctc.org

November 2005

2-4: **CPM 2005 EAST**
Orlando, FL
Web: www.contingencyplanningexpo.com

December 2005

6-8: **CPM 2005 CANADA**
Vancouver, BC
Web: www.contingencyplanningexpo.com

Limited Time

Special Subscription Offer

YES! Send me the next 12 issues of *CPM Global Assurance E-Newsletter* at the special subscription price of $149 — a savings of almost $50 off the charter rate of $195.

Complete and mail or fax to:
CPM Global Assurance E-Newsletter
Witter Publishing Corp.
20 Commerce St., Suite 2013
Flemington, NJ 08822 USA
908 788-0343 • Fax 908 788-4209

www.ContingencyPlanning.com

Priority Code: 05GA07

❐ My check for $149, payable to Witter Publishing Corp., is enclosed.

Charge $149 to my:
❐ VISA ❐ MasterCard ❐ American Express ❐ Discover Card

Account: |__|__|__|__|__|__|__|__|__|__|__|__|__|__|__|__| Exp:______

Signature:____
(Required for all orders)

Name:____

Title: ____

Company:____

Address 1: ____

Address 2: ____

City/County/Province: ________________________________

Zip/Postal Code: _________Country: ____________________

Phone: ____________________ Fax: ____________________

*E-mail: ____
(required)

Spring into action and learn to save your organization! CPM 2005 EAST is the must-attend event for business continuity/COOP, emergency management and security professionals. Sessions include:

- Transforming your Company into a Resilient Business
- Mission Critical Facility Protection
- Protecting Corporate Assets
- Mach 5: High Speed Training Program
- More Case Studies than ever!

Register Now!
www.ContingencyPlanningExpo.com

Gaylord Palms Resort
Orlando, FL
November 2-4, 2005