Volume 2 • Issue 1
January 2005

CPM Global Assurance
Integrating Business Continuity, Security, and Emergency Management

CONTENTS

January 2005 Issue

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!

Moving From "If" to "When"

Addressing the Urgency of Business Continuity Management

By Steven Ross and Paul Kirvan

This article was developed from results of the 2004 Benchmark Survey of Business Continuity jointly conducted by The CPM Group and Deloitte & Touche, LLP.

The best approach to disaster recovery and business continuity management might be found in this simple semantic exercise: Change "if" to "when."

In other words, adjusting the mindset from "*if* disaster strikes …" to "*when* disaster strikes … ," can give the issues of recovery and continuity a new — and proper — urgency.

But is this a case of unwarranted fear-mongering? Are we needlessly raising the specter of a business-fixated bogeyman? A British study suggests otherwise: According to a recent report in the Times of London, one in five small businesses suffers some sort of severe disruption each year. Even more sobering: Computer Weekly magazine states that 60 percent of businesses that endure a catastrophic fire or flood — and don't have a disaster recovery and business continuity management plan in place — *never* recover.

Fortunately, there are signs that executives are getting the message. A recent study by Deloitte & Touche LLP and The CPM Group reveals that 50 percent of surveyed companies have implemented corporate business continuity plans, compared to only 30 percent five years ago. And according to a survey by Millward Brown IntelliQuest, improving business continuity management (BCM) currently ranks as the third-highest priority for U.S. businesses.

But if the Deloitte / CPM study shows that 50 percent of companies have implemented BCM plans — what about the other half? What is holding them back? The underlying factors are diverse:

- **Denial mentality:** Many executives — especially those headquartered outside of major urban areas — operate under the quaint (and still popular) notion of "it can't happen here." They may believe that serious threats only apply to the high-profile, multinational corporations of the world. Or they may think that a company in the heartland faces few dangers, conveniently forgetting that chemical manufacturers, airports, nuclear power plants, and other high-risk facilities are sprinkled throughout the country.
- **Underestimated threats:** A significant segment of executives associate BCM with terrorism and little else. But in fact, any number of threats could jeopardize a company's operations, including computer viruses and hacking; blackouts; fires; earthquakes; hurricanes, floods, and other

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

Production
Production Manager: MIKE VISCEL, ext. 122
MViscel@WitterPublishing.com

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

Subscriptions
Circulation: COURTNEY WITTER, ext. 132
CWitter@WitterPublishing.com

Reprints
PR Reprint Marketing, 800 992-7137
sales@reprintmarketing.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. 171
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"

weather-related events; accidents; incapacitation of key personnel; and much more.

- **Misplaced priorities:** Many executives acknowledge the need for disaster recovery and business continuity planning, but they don't rank it as high on their to-do list as other pressing business issues.
- **Insular perspective:** A company that has trained its people, backed up its data, and placed fire extinguishers strategically throughout its plant may believe it has a viable plan in place. But many hazards exist on the other side of the corporate firewall. Consider the implications of a key supplier or a major customer going bankrupt, for example.
- **Cost concerns:** Many executives labor under the misconception that business continuity will be expensive and resource intensive. Yet those who initiate their program with a comprehensive risk assessment and thorough business impact analysis quickly learn the financial requirements aren't nearly so onerous.

> "Adjusting the mindset from "if disaster strikes …" to "when disaster strikes … ," can give the issues of recovery and continuity a new — and proper — urgency."

After an examination of companies that have failed to implement business continuity management plans, it is equally instructive to consider what compelled the other 50 percent to act. Here, again, the root causes are varied:

- **Regulatory compulsion:** Certain highly regulated industries — including banking and other financial services, insurance, and telecommunications — are required by law to have viable disaster recovery and business continuity plans in place. Sarbanes-Oxley, Graham-Leach-Bliley, and other legislation will likely accelerate this trend.
- **Need recognition:** In the Deloitte & Touche / CPM survey, 34 percent of executives stated that they initiated a BCM program at their company because management had recognized business continuity as a serious problem requiring prompt attention. Another 17 percent cited the process of risk management as a primary driver.
- **Stakeholder protection:** The desire to safeguard the investments of shareholders spurred 12 percent of executives surveyed to adopt a BCM program.

One final survey result: Nine percent of the executives in the Deloitte & Touche / CPM survey said they were burned once through a severe business disruption and took steps not to suffer the same fate again. Although these executives perceived the shift from "if" to "when" a little too late, they now realize the indispensable need for disaster recovery and business continuity planning.

The future of business in North America – and worldwide – is likely to include more, not less, disruptive situations that will challenge management. And while it's clear – and regrettable – that fifty percent of U.S. executives have yet to attain a similar insight, we must increase our willingness to move beyond our traditional comfort zones and accept the fact that proper corporate governance in the 21st century includes business continuity management. ■

About the Authors

Steven Ross is a director with Deloitte & Touche LLP; Paul Kirvan is editor-in-chief of CPM Global Assurance.

The views expressed in this article are those of the authors, and not necessarily the views of Deloitte & Touche LLP.

Xand Launches Successful Seminar Series for SME Market

Xand Corporation (Hawthorne, NY) recently launched the first in a series of half-day seminars addressing the need for business continuity to the small to medium enterprise (SME) business market. The program featured speakers in business continuity and insurance who discussed issues about business survival facing SMEs today. Of particular interest were discussions on selecting business and liability insurance, conducting BC activities on a limited budget, why business continuity should be a part of strategic planning, and why it should be a part of corporate culture. Additional seminars are being planned; to find out more contact *www.xand.com*.

New Website Links Canadian Small Business Owners and Entrepreneurs

Making the right alliances is vital to succeeding in business, and for small businesses it can be critical. Partnering and joint ventures help companies create new products and / or services, and to make inroads into new markets. Business Partnerships Canada (Toronto, ON) is a new forum for introducing small business owners to other entrepreneurs, jointly developed by Alleyne Inc. (Toronto, ON) and pixcode Inc. (Toronto, ON). Site members know that other members are people who are open to meeting business owners, and more importantly, they can see what the other members are offering and hoping to receive in return. Each member can indicate whether he or she is looking for opportunities in partnering or bartering, or looking to form a "Creative Intelligence" alliance. This is also an excellent way of introducing business continuity, security and emergency management to the small to medium-sized business community. *http://BusinessPartnerships.ca; www.pixcode.com*; *www.alleyneinc.com*

NEDRIX and CPM Hold Joint Symposia Event in Boston

The New England Disaster Recovery Information Exchange (NEDRIX), based in the Boston area, in collaboration with CPM, held a successful one-day conference on the strategic integration of business continuity, security and emergency management. After a morning of sessions addressing strategic and outside-the-box issues for business continuity, security (physical and information), and emergency management, the 70 delegates worked through an afternoon workshop in which they developed plans for introducing a plan to integrate the disciplines into their own companies. Additional programs are planned in 2005. For details go to *www.contingencyplanning.com* or contact CPM's editor.

Peak 10, Arsenal Announce Partnership

CARY, NC, November 15, 2004 Arsenal Digital Solutions (Cary, NC) a storage management services (SMS) provider, recently announced a partnership with Peak 10 (Charlotte, NC), a Southeastern data center and managed services provider. The partnership strengthens Peak 10's data protection and backup / restore services through Arsenal's ViaRemote(tm) and ViaManage(tm) offerings. Arsenal's ViaRemote is a network-based data backup and recovery service that provides secure, bandwidth-efficient, disk-based backup / restore over the Internet or private network. This product enhances Peak 10's remote data protection service by helping its customers back up data from any location over their existing network to any one of Peak 10's five secure data center facilities. Peak 10 enhances its ability to monitor and manage its existing tape backup and restore services through Arsenal's ViaManage offering, which combines advanced monitoring and reporting services with complete management and resolution capabilities. *www.arsenaldigital.com; www.peak10.com*

Law Firm Selects XOsoft's WANSyncHA(tm) for Continuous Server Availability

XOsoft (Burlington, MA), a provider of continuous application availability software solutions, recently announced that Pillsbury Winthrop LLP, an international law firm with over 750 lawyers in 16 offices located in the United States, London, Australia and Asia, relies heavily on its Microsoft Exchange-based messaging infrastructure to remain in constant touch with its customers. The firm also requires the highest availability of its Microsoft SQL-based iManage application suite, which hosts legal documents and contracts. To maintain its customer relationship management standards, both platforms must be on-line at all times. The firm has deployed WANSyncHA Exchange and WANSyncHA SQL on Microsoft Exchange and SQL servers at its Los Angeles, San Francisco, New York and Washington, DC offices. This setup enables replication and continuous synchronization of the firm's Exchange and iManage application servers. In case of disaster, servers at the Washington, DC offices are configured to act as a failover site for servers at both West Coast offices, while servers at the San Francisco offices are configured to act as a failover site for servers at both East Coast offices. *www.xosoft.com*

Hitachi Data Systems Announces Compatibility with IBM Enterprise Systems

Hitachi Data Systems Corporation (Santa Clara, CA), a wholly owned subsidiary of Hitachi, recently announced the completion of interoperability tests between the IBM's TotalStorage Enterprise Storage Server Series and Hitachi's TagmaStore(tm) Universal Storage Platform. Storage virtualization simplifies the management of storage and data resources in a time of accelerating storage demand and functional complexity. Hitachi

TagmaStore Universal Storage Platform now adds IBM TotalStorage Enterprise Storage Server Models 750, 800 and 800 turbo as supported storage devices. *www.hds.com*

Study: Sarbanes-Oxley Compliance Costs Average $16 Million Per Company

A survey of corporate boards released today by RHR International (New York, NY) and The Directorship Search Group (New York, NY) revealed that Sarbanes-Oxley compliance costs averaged $16 million annually – a jump of 77 percent from last year. Findings of the first annual Directorship / RHR International Board Survey also reveal that nearly half (47 percent) of companies surveyed do not have a CEO successor in place, although 61 percent expect that CEO leadership transition will go smoothly, according to the poll of almost 270 board directors at U.S. companies. Of the 266 board directors surveyed, almost two-thirds (64 percent) reported that the new regulations have changed their participation as a director. One major change is highlighted in the compensation of the company CEO. Nearly two-thirds (63 percent) of the directors indicated plans to change either the CEO salary or salary relative to bonus. *www.directorship.com; www.rhrinternational.com*

ACP Launches Second Chapter in Tennessee

The Association of Contingency Planners (ACP) has announced its newest chapter, the Mid-South Chapter, located in Tennessee. The ACP now has two chapters in Tennessee: Mid-Tennessee in Nashville and Mid-South in Memphis. The Mid-South Chapter President is Glen Curole, who can be reached at (901) 419-5047 or glen.curole@ipaper.com. *www.acp-international.org*

Kenyon International Implements National Notification Network Solution

National Notification Network (Glendale, CA), a provider of mass notification systems, recently announced that Kenyon International, the industry leader in disaster and mass fatality management, has selected the 3n Mass Notification System to coordinate deployment of Kenyon disaster response / recovery teams worldwide. Kenyon needed a system capable of immediately delivering notifications when called to an accident or act of terrorism. Deployment notification currently originates from Kenyon's Houston, TX headquarters. The 3n system will improve communications with the more than 1,000 team members who form the nucleus of Kenyon's disaster response teams. Based on instructions from the Kenyon administrator, the 3n system will distribute a pre-prepared voice or text message to all phone numbers and email addresses in the Kenyon database. The messages instantly inform team members of a disaster and provide emergency instructions and updates, and can be relayed to all modes of communication used by recipients, including phone (home, work, cell), email, pager, fax and wireless devices such as laptops, PDAs and BlackBerries. *www.3nonline.com*

Emergency School Notifications Handled via SMS

When a disaster or any emergency situation arises, and a large group of people needs to be contacted instantly and reliably: parents, teachers, emergency services, community, Family First Alerts by Chatter (San Diego, CA) provide schools with emergency alert services via SMS (short message service) technology. The service lets school officials send time-critical alerts to one or thousands of individuals instantly and reliably using a computer or a cell phone from any location. After an emergency situation occurs, phone lines, Internet access, electricity and other communications tools might be out of service. It is important to know that any mobile device (e.g., cell phone) is capable of receiving a text message more reliably than a voice message. This is because the technology is more resilient under conditions of poor transmission. Family First Alerts inform parents of an evacuation, and then advises them what to do next. After-the-event information can be disseminated in a targeted manner. *www.familyfirstalerts.com*

Discover the Synergy Among Business Continuity, Emergency Management and Security

Register for CPM 2005 West, May 24-26, 2005 in Las Vegas for an expanded focus on education and leadership within the business continuity, emergency management, and security disciplines. International affairs expert and NBC military analyst General Barry McCaffrey will deliver the keynote address. New course content, dynamic speakers, effective networking events and more make CPM 2005 West the one conference and exhibition to attend for continuity, security and emergency management. Register at *www.ContingencyPlanningExpo.com* ■

International News

www.continuitycentral.com

Public Consultation Launched on UK Civil Contingencies Act

Cabinet Office Minister Ruth Kelly recently announced a solicitation for public comment on the draft regulations and guidance accompanying Part One of the Civil Contingencies Act 2004. The Act provides the framework for civil protection in the UK. Part One deals specifically with local civil protection arrangements, and imposes specific business continuity responsibilities on local government authorities and other agencies and the draft regulations and guidance documents provide added detail on what is expected in these areas. Minister Kelly said, "The Civil Contingencies Act emphasizes the government's commitment to improving the resilience of the UK. I urge practitioners to feed their views back to us. I hope the launch will also serve as a prompt to encourage organizations to think about the challenges of implementation in order to improve their ability to deal with consequences of major disruptive incidents." Consultation documents are available at *http://www.ukresilience.info/ccact/index.htm* and will run until March 3, 2005. Continuity Central is launching a new website, *http://www.civilcontingenciesact.co.uk*, as an information resource for the Civil Contingencies Act.

Aladdin Identifies Potential Mega Virus Related to JPEG Vulnerability

Aladdin Knowledge Systems (Tel Aviv, Israel) recently announced it has identified a potential 'mega virus' stemming from a recent JPEG vulnerability. Aladdin content security specialists based in Haifa, Israel have pinpointed three scenarios that could lead to a wide-spreading virus affecting organizations around the globe: 1) email attachments, 2) images on a Web page, and 3) email with a linked image. Infected images could reside not only on Web servers prepared by attackers, but also on previously infected computers which are now turned into slim Web servers or on infected Web servers. This is similar to Nimda and other worms that infected Microsoft IIS Web servers. Aladdin recommends that organizations adopt the following six action steps to reduce the chance of this threat occurring:

1. Don't rely on SMTP or internal mail server content inspection. A complete solution must be a gateway solution and must inspect HTTP and FTP in addition to SMTP.
2. Identification of JPEG files should not rely on extensions, or content type, to prevent spoofing.
3. JPEG files should be inspected packet-by-packet in real time to eliminate latency. Users should not have to wait until the entire file is downloaded and inspected by the proxy.
4. All parts of the JPEG file must be fully inspected before being released to the client. Solutions cannot rely on partially releasing non-inspected content.
5. The gateway solution must not pose any delays and timeouts or create any visible impact on users' browsing experience – either when cached JPEG files are delivered or when new images are downloaded.
6. For hosted web sites that allow file uploads, inspect all uploaded JPEG files.

http://www.ealaddin.com

U.S. and U.K. to Jointly Develop Risk Assessment Methods for Critical Infrastructure Protection

During a recent meeting of the fourth Joint Contact Group, U.K. Home Secretary David Blunkett and U.S. Homeland Security Deputy Secretary James Loy signed a Memorandum of Agreement establishing a framework for cooperation in science and technology in critical infrastructure protection and other homeland / civil security concerns. They issued the following joint statement: "We are pleased to announce the signing of the Science and Technology Agreement, which outlines formal U.K.– U.S. arrangements for future cooperation in the area of science and technology research and development. This agreement demonstrates the strong relationship between the U.K. and U.S. and supports exchanges of homeland / civil security information, development of threat and vulnerability assessments; development and exchange of commercially adaptable best practices, standards, and guidelines; development, testing, and evaluation of Homeland / civil security technologies; and utilization of each country's respective research, development, testing and evaluation capacities".

Disaster Recovery Put to Test in South Africa

In Johannesburg, central securities depository Strate recently consolidated its disaster recovery process and at the same time reduced its recovery window from eight hours to one. Strate is also an electronic settlement house, and without an adequate disaster recovery process, settlement of trades in equities and bonds could suffer serious setbacks. Until recently, Strate's disaster recovery environment was spread over three sites, using mostly outsourced equipment with a recovery window of up to eight hours for the entire infrastructure. Another challenge was that the high availability solution was too close to the production facility, with one mainframe housed only 100 meters from the backup mainframe. Strate consolidated the three sites into one, in consultation with business partners Business Connexion, SunGard and Telkom. All critical production site data is now mirrored to the recovery center on a real-time basis via Telkom's LAN-Connect solution. The new arrangement was recently put to the test when Strate experienced a municipal power problem at its Illovo offices. Employees were relocated to the disaster recovery site where they performed their settlement functions for the day, with market participants unaware of any problems.

Financial Insights Estimates Cost of Basel II for Banks in Asia/Pacific Region

A recent report by the research and advisory firm Financial Insights discusses the payoffs of Basel II compliance and quantifies the corresponding investment on IT systems and interfaces in Asia. Entitled *Basel II, Chapter 1: The Cost of Compliance in Asia/Pacific*, the report also analyzes strategic considerations that provide the impetus for software solutions vendor selection. "The allure of the Basel II accord is multifaceted, having evolved from a single, simplified step into a comprehensive program for risk improvement. Tenets of superior risk management include processes for risk identification, assessment of threats to solvency posed by the risks uncovered, and the discipline to manage the risks to prevent them from rising unduly high," according to Li-May Chew, CFA and senior research manager for Financial Insights' Asia/Pacific Capital Markets Advisory Service. For more information on this report, send an email to sang@idc.com.

CBL Expands Data Recovery Facilities In Brazil

CBL Data Recovery Technologies Inc. (Armonk, NY), an international provider of computer data recovery services, has expanded its laboratory facilities in Curitiba, Brazil to meet the ever-increasing data recovery needs of the region. The growth of CBL's Brazilian data recovery operations follows closely the company's recent expansion in San Diego, California and Singapore, as well as the opening of a data recovery lab in Japan. "Clearly there was a need to expand our data recovery operations to meet growing demands in Brazil and all of South America," said CEO Bill Margeson. "Time is a critical factor when providing data recovery services, so enlarging our physical presence in the region enables us to better serve customers in a prompt, efficient manner." *www.cbltech.com*

Singapore Takes Lead in BC Supplier Certification

The Infocomm Development Authority of Singapore (IDA) has announced that Singapore's industry-led Business Continuity / Disaster Recovery Working Group of the Information Technology Standards Committee (ITSC) has developed the world's first industry standard for business continuity and disaster recovery service providers. The industry standard specifies stringent requirements that business continuity and disaster recovery service providers must demonstrate so that they can provide a trusted operating environment and help companies secure and recover critical data in a crisis. These requirements include stipulations for operating, monitoring, maintaining and up-keeping business continuity and disaster recovery client services. The standard will serve to differentiate between service providers and help provide guidance for end-user companies in choosing the most suitable providers. **S**even companies have already received certificates of compliance with the new standard: Hewlett Packard, IBM, NCS and Singapore Computer Systems (business continuity and disaster recovery service providers); and Equinix, SingTel and StarHub (disaster recovery facilities). ■
www.idanews.gov.sg

GLOBAL ASSURANCE PRODUCTS

New Integrated Information System Streamlines Data Management for Risk Management Firms

Wramsco (Lisle, IL) an independent risk and claim management firm, has announced its new WIN System, an integrated online network system for real-time risk management, claim management and data manipulation. The firm claims the system has the ability to reduce claim loss costs by 40 to 60 percent. The WIN System allows information in eight modules to be accessed and retrieved in real time from any location that is connected to the system. Key elements in the system include the Client Module, Claims Management Module, Adjuster Module, Financial Module, Medical Module, Litigation Module, Multimedia and Research Module, and the Underwriting Module. Existing risk management systems can be integrated into the WIN System. It works within an advanced firewall system, has on-site and off-site redundant backup, and a nationwide network infrastructure using Intel Xeon based servers with 128-bit encryption. Wramsco offers 24/7 technical support.
http://www.wramsco.com

CNT's UltraNet Edge Storage Router Certified as IBM TotalStorage Proven

CNT (Minneapolis, MN), a provider of storage networking solutions, announced that its UltraNet Edge Storage Router has successfully completed interoperability testing with IBM's Enhanced Remote Mirroring for DS4000 products and has been certified as IBM® TotalStorage Proven(tm). The IBM TotalStorage Proven program builds on IBM's interoperability efforts to develop and deliver products and solutions that work together with third party products. The UltraNet Edge Storage Router interconnects and extends Fibre Channel and FICON® data center networks across campus or across the globe, enabling flexible, cost-effective, enterprise-wide storage infrastructures that improve data availability and make business continuity achievable. The UltraNet Edge Storage Router manages the long-distance connection and provides maximum throughput and complete data integrity. *www.cnt.com*

GLOBAL ASSURANCE PRODUCTS

American Power Conversion's New Mobile Data Center Available Now

American Power Conversion (West Kingston, RI) recently announced the availability of InfraStruXure Express, a fully mobile data center for businesses working on transitional IT projects or developing robust business continuity and disaster recovery programs. Based on APC's InfraStruXure architecture, InfraStruXure Express features a highly available Tier IV (redundant power and cooling) data center design that is self-contained and can be populated with standard IT equipment such as servers and internetworking gear. The solution requires no existing indoor IT real estate or prep work at the client site, and can be immediately deployed from in-stock components. This approach is also ideal for data centers that are undergoing transitions such as server migration / consolidation, moves / adds / changes, construction / restructuring or technology adoption. The InfraStruXure Express accommodates up to eight individuals (two seating areas). The structure supports connections for voice, data and entertainment. The specialty trailer is a heavy-duty, regulation size drop frame designed for electronics and is 53 feet long, 8 ½ feet wide and 13 ½ feet tall (permissible vehicle dimensions meet DOT regulations). InfraStruXure Express is currently available in North America for purchase or lease. Customers can order this solution as an IT data center infrastructure or preloaded with customized equipment. *www.apc.com*

PowerFlare, the Ultimate Safety and Sport Light

Safety lighting and signals for normal and emergency applications are available from PowerFlare Corporation (San Jose, CA). Invented by a police officer, the PowerFlare electronic beacon is a bright and rugged, military-grade safety device that is designed to replace incendiary flares and provide sport and safety lighting. Two versions are available. The non-rechargeable version uses a sealed lithium cell "LC" unit that lasts for up to five years, features a single-blink "strobe" flash pattern, and runs up to 100 hours. It can be keep in auto trunks or in first aid kits, and can serve as a rescue beacon for boats, planes, etc. The unit price is $39.95. The rechargeable 1-pack system has five user-selectable flash patterns as well as solid-on for lantern applications, and features a cell phone-type car charger; a magnetic switch; and the unit is rated to 300 feet under water. Applications include cycling, hiking, camping and SCUBA. The unit price is $89.95. *www.powerflare.com*

New Software Addresses Sarbanes-Oxley Compliance

BizNet Software, Inc. (Dallas, TX), which combines accounting and technology expertise to help companies improve financial reporting and processes, has announced BizNet Insight for Compliance, a solution that helps companies improve Sarbanes-Oxley compliance initiatives with minimal change to their existing procedures. The product lets enterprises port their existing procedures created for first-year compliance and implement an ongoing compliance process at a reasonable cost that is sustainable on an ongoing basis. BizNet Insight for Compliance is an integrated system that supports efficient knowledge management, workflow, control documentation, risk assessment, information sharing and status reporting. The product uses Microsoft Office technologies to increase an organization's productivity and decrease training needs. Built by accountants, BizNet Insight for Compliance helps accounting and financial professionals improve internal controls, automate current processes, and gain efficiencies in compliance reporting. *www.biznetsoftware.com*

PPM 2000 Updates Tool for Incident Reporting

PPM 2000, Inc. (Edmonton, Alberta, Canada), a developer of security management solutions, recently unveiled a new release of IXO, the firm's web-based incident reporting system. In addition to its standard real-time access to incident information, IXO Plus offers includes editable field labels, user-defined fields, and support for multiple languages concurrently. *www.ppm2000.com*

The Unexpected Benefits of Good Business Continuity

By Andrew McCrackan

At CPM we're always looking for new approaches to the business continuity process. Through our friends at Continuity Central we're pleased to introduce Andrew McCrackan, author of a new book and methodology on business continuity. – Editor

For many organizations the cost of comprehensive business continuity and disaster recovery programs can be significant. Few realize that the benefits of a business continuity management program extend far beyond the ability to recover from unpleasant events.

In order to determine continuity related risks, critical business processes and critical resources as part of the business impact analysis (BIA) process it is necessary to analyze the subject organization in some detail. For many organizations this sort of scrutiny, extending across every aspect of the business, will never have been done before. The discoveries made as a result of business continuity related analyses could come as quite a sur-

prise to executive managers.

It is often the case that an unexpected output of the BIA process is the identification of opportunities to enhance, through optimization or rationalization, various high-level and low-level business processes. Firms may realize that they have duplicate functions or functions which overlap. They may identify illogical workflows or, in more cases than you could imagine, evidence that the organizational model itself is not fit for purpose due to such factors as segmentation and misalignment with core business processes.

While such issues are often set aside as "out of scope" or passed to others to address, it should be realized that these outputs are not side effects of the business continuity management process but are fundamentally important outputs of the process. Indeed, the business efficiencies that can be achieved through addressing such identified issues can be significant. These efficiencies can be so substantial that the benefits may be used to cost justify a significant portion of the business continuity program. The benefits are also great publicity for a business continuity initiative because they are often simple to relate to stakeholders and are seen as particularly tangible in terms of the day-to-day business of the firm.

While a business continuity cost offset is a great thing to have, it needs to be better understood that in holistic business continuity terms, the rationalization of business processes can be seen as a necessary step in building organizational resilience. A poorly defined and inefficient process is usually more prone to failure than a well thought out and optimized one. Poorly defined processes can also be more complicated than optimized processes. As is the case with technology systems, an overly complex process is more difficult to successfully replicate or recover than a more streamlined one. Simply put, complexity of process is inversely proportional to probability of successful recovery in a crisis or disaster situation.

The most common and fundamental example of this issue is significant misalignment of the firm with its critical business processes. For all types of business it is possible to create a normalized model, which essentially represents the core business process at its most fundamental level. In a manufacturing company, for example, this may consist of several steps such as product development, marketing, sales, procurement, production, logistics, billing and customer care. As you can see these essentially represent the business lifecycle. We design the product, market it, receive orders, build it, deliver it to the customer and bill them for it, and we also look after the customer in terms of post-sales support. From this fairly obvious business model we can arrive at the top layer of the organizational structure. More detailed analysis of the business plan will reveal the necessary lower layers of the structure. Across this we map some standard support and governance functions and we have our complete structure. While this seems fairly obvious I have rarely found an organization that has recently had a meaningful discussion about the design of their structure. Most structures simply grow organically over extended periods of time until no one exists anymore that remembers why or how the structure was designed. The larger the business, the more prevalent this problem can be.

The associated risks with this scenario arise largely from a lack of definition around communication, authority and responsibility, and can result in the failure of critical business processes, thus impacting the overall continuity of the business. If such issues are identified as part of business impact analysis efforts then these should be addressed as part of the subsequent strategy, with changes or controls being put in place prior to the implementation of recovery capabilities. A lean, optimized firm is generally more robust and resilient in a crisis situation.

We are all familiar with the saying about the "left hand not knowing what the right hand is doing". This saying was born out of the prevalence of this issue and is most frequently used when referring to government agencies and large-scale corporations. It describes the business continuity risks associated with poor organizational and business process design. In the case of government, efficiency gains arising out of business continuity management efforts should be particularly welcome. Optimizing the machinery of government may not only reduce the impact of an event on our critical community infrastructure, but could have the unexpected benefit of lowering taxes through increased process efficiency! ■

About the Author

Andrew McCrackan is the author of *A Practical Guide to Business Continuity Assurance*, Artech House, Boston, 2004. He is also founder and principal consultant of Continuity Assurance International, based in the UK. *www.continuityassurance.com*

Vital Records Protection at the Municipal Level

■ **By Van Carlisle**

It goes without saying that all levels of government should be prepared to protect vital public records against fire, flood or any other type of disaster. From the U.S. Constitution to a simple parking ticket, important and vital governmental documents should be kept in fireproof file cabinets, safes or vaults. Federal, state and local governments should all have their own specific rules and regulations when it comes to vital records protection. While vital records protection at the state and federal level is regularly addressed and heavily regulated, things are different at the smaller city and town levels.

The town of Cape Carteret on the coast of North Carolina

is subject to state regulations regarding records protection because of its proximity to the ocean and the possibility of a hurricane hitting the coast, devastating buildings and destroying everything in its path, including important files and documents. Carol Fox, deputy clerk for Cape Carteret said that "Minutes from the bi-monthly board meetings, personnel records, financial documents, historic town maps, and other permanent records are kept in our four fireproof file cabinets. Thankfully, we purchased these proactively rather than reactively to a disaster where we could have lost very important municipal documents."

Unfortunately, not all municipalities have regulations on what needs to be protected and the method of protection. For example, the small town of Elida, NM, with less than 500 residents, does not have any local, state or federal rules on vital record protection. According to Sandra Monks, Elida's Town Clerk, traffic citations and other important court correspondence are kept in a fireproof file.

On the other end of the spectrum, some local government offices keep all records in UL (Underwriter's Laboratory)-rated fireproof file cabinets. Underwriters Laboratories Inc. (UL) is an independent, not-for-profit product safety testing and certification organization that tests products for public safety. Fireproof file cabinets and safes with the "UL-rated" seal have been tested and passed according to UL's specifications.

When a disaster destroys documents it makes proactive protection a very wise decision, whether by law or choice. Fran Leal, office manager for the town of Sterling in northwest Illinois, endorses the protection of all office documents. "Here in Sterling, all of our office documents are kept in fireproof file cabinets," she said. "Also, any of our non-essential daily documents are backed up on disks, which are in turn stored in fireproof containers. It gives us peace of mind knowing that the documents are secure and will not need to be replaced following a disaster."

Not all municipalities have been so lucky. In April 2002 a devastating fire destroyed nearly everything in the municipal offices of Ovid, CO. The only items salvaged were those that were stored in the fireproof safes in use at the time. "It was a huge mess. We were not properly prepared or protected at all. Thousands of important documents were gone forever after that day," commented Carol Dunker, Ovid Town Clerk.

A more recent example of a town losing almost everything due to fire damage happened on May 27, 2003. The municipal building in Doniphan, MO housed the town clerk, courthouse, mayor's office, police station and prison. On that particular day, a prisoner stuck a piece of lead in a socket to create a flame for the purpose of lighting a cigarette. A few moments later the fire in the walls behind the socket spread throughout the building, which would eventually cause major structural damage. Barbara Jarrett, Doniphan City Clerk at the time, spoke about the damage caused by the prisoner. "It was a real disaster. All of the prisoners had to be relocated to another facility while the fire ravaged the building. After the fire was extinguished and we could assess the actual damage, we found that about 95% of all the documents had been destroyed. Even the ones in the fireproof containers were badly damaged because of smoke and water entering the container."

Mayor William Rosenblatt, Loch Arbour, NJ, understands the need for vital record protection. "Although we have never lost any documents because of a fire, I fully appreciated the need for a way to secure them," he said. "Document recovery can prove to be an impossible task after a disaster. I've been mayor of this small town for nearly ten years and can only imagine the amount of work that would be required to restore or replace some of the documents that can be as old as 50 years. In my opinion every office, not just a governmental office should take whatever measures necessary to protect their most vital records."

Whether local, state or federal, all governmental agencies and municipalities should be prepared and protected for a disaster of any kind. Keeping records secure and intact is essential to moving forward following a catastrophe. ■

About the Author

Van Carlisle is President and CEO of Fire King, a security and loss prevention company.

Underwriters Laboratories Inc. (UL) is an independent, not-for-profit product safety testing and certification organization that tests products for public safety. *www.ul.com*

Selecting a Disaster Restoration Provider

By Bob Vanchure

Thousands of commercial and industrial buildings are damaged each year by unforeseen disasters, ranging from fire or smoke and soot to water that infiltrates walls, floors, and equipment through burst water pipes, seepage, fire sprinkler flooding or leaks from a rainstorm.

Potential risks include destruction of interior structural materials, equipment and files; disruption of operations; damage from humidity; and, if water is not removed quickly, microbial damage, e.g., mold, a potential health hazard. Wherever such an event occurs, the results can be operationally and financially disastrous.

When damage occurs, immediate action is necessary to stabilize the loss and mitigate damage. Doing so will maximize recovery of all contents such as inventory, machinery, furniture, carpeting, electronic media, documents and files; and will minimize replacement costs, preserve good indoor air quality, and control mold risks.

Advance Planning

The best "insurance" in a recovery situation is to plan in advance of an occurrence by creating a disaster recovery plan (DRP). Next, pre-selecting a full service restoration provider ensures that building owners and managers will have a "partner" in the reclamation process. Select a restoration provider that offers guaranteed priority emergency services. In the event of a fire, weather-related or other water-damage disaster to a building or facility, owners or property managers registered in these programs will receive immediate priority for emergency drying and restoration services.

Expectations

Following is a list of services you should expect from the restoration company:

- Consulting. The project scope should be provided at the front end. The firm quantifies the damage, determines what can be saved, recommends the equipment and process and confirms results through independent testing.
- Project Management. The company has the ability to quickly assemble a suitable work team, provide rapid emergency response, and provide a turnkey operation for recovery, restoration, and guaranteed results.
- Stabilization. The provider stabilizes the environment and assists with relocation efforts to an unaffected area or off-site, if necessary.
- Dehumidification and Drying. Through removal of standing water and excess moisture, the firm has the ability to reduce material loss, limit indoor air quality problems and speed return to occupancy and operation of the affected business.
- Cleaning and Disinfecting. By cleaning, sanitizing and disinfecting interior surfaces, the provider eliminates contamination from molds, bacteria, mildew and potential biological hazards.
- Odor Control. Thermo fog, wet spray, ozone or dry vapor methods should be properly employed to control odor.
- Electronic Equipment Restoration. In many cases, it is possible to clean and restore high-tech components following exposure to fire or water damage.
- Preservation of Large-Scale Production Equipment. Contamination removal preserves operating equipment such as printing and hydraulic presses.
- Document and Media Restoration. Cleaning, sanitizing, deodorizing and drying restores paper records and electronic media storage such as magnetic reels and floppy disks. This process is most effective if the firm dry cleans by vacuum and has refrigerated transport storage capabilities so that material deterioration can be minimized.
- HVAC and Mechanical Systems Cleaning. Cleaning and deodorizing the supply and return duct system as well as the metal housing that encloses coils, heat exchangers and filter banks ensures that clean air again passes through the system.
- Smoke and Water Decontamination. Residue from damage sources such as fire, flood and storms is removed.
- Corrosion Control. Metal surfaces are cleaned and treated to prevent further damage from corrosion.
- Controlled Demolition and Disposal. Surfaces that will not respond to restoration efforts in a cost-effective way are removed to expose hidden cavities and to expedite the recovery process or to remove sources of odor.

Selecting the Right Firm

When researching cleaning and restoration technicians, a list of providers can be obtained from an organization such as the Property Loss Research Bureau (PLRB) *www.plrb.com*. Also, review Web sites; read case histories on the site; and contact company representatives. The assessment process begins with reviewing experience, reputation and references. Ask the following questions of reference sources:

- What was your problem and what results did the restoration service achieve?
- Did they provide a written scope of work and budget?
- Did they quantify the damage to limit the recovery effort to the affected areas of the structure?
- Do they guarantee their work in writing?
- Do they provide turnkey service, ranging from consulting and engineering to drying and restoration?
- Do they have vacuum freeze dry, desiccant dry chamber, blast freezing and refrigerated transportation and storage capabilities?
- Do they offer Web site monitoring of drying equipment?

- What was their response time to you?
- Do they have a local office in your area?
- Were they on budget?
- Were you pleased with them and would you use their services again?
- Would you recommend them to work with another company?

Moisture damage in buildings manifests itself in extremes that range from simply too much humidity or water intrusion that encourages mold to extreme cases where major flooding threatens the structure. As can be seen from the case study, the impact from a natural or man-made disaster can be minimized through advanced planning, emergency response team training and working with a professional disaster restoration provider. ■

About the Author

Bob Vanchure is Regional Sales Manager for Munters Moisture Control Services (MCS), based in Amesbury, MA. MCS is a full-service water damage recovery / temporary humidity control company, providing emergency services through 30 offices in the U.S. and Canada.

Public- and Private-Sector Wireless Vulnerabilities

■ **By Bob Brewin and Frank Tiboni**

A survey of wireless security in the Washington area during October 2004 found that Wi-Fi networks at several federal agencies and defense contractors did not meet the security policies issued by Defense Department officials in April 2004 or guidelines issued by National Institute of Standards and Technology (NIST) officials in November 2002.

For example, at CSC's federal division campus in Falls Church, VA., FCW reporters discovered five rogue, or unauthorized, wireless access points. During the tour, the reporters detected a wireless bridge at the headquarters of the Defense Information Systems Agency on Courthouse Road in Arlington, VA, which was transmitting megabytes of traffic.

Open to trouble

Wireless networks often can be detected because many access points have a built-in beacon function. That function broadcasts a signal known as a Service Set Identifier (SSID) to make it easier for wireless devices to find the link. However, it is also a beacon for hackers looking for an entry point into an organization's network. As part of their guidelines, NIST officials suggest agencies turn off the built-in function. Even with the broadcast function turned off, SSIDs are transmitted in other frames of the Wi-Fi signal, which can be detected by sniffing software. NIST recommends agency officials use an SSID that does not reveal information about the agency, such as name, division or department.

FCW detected hundreds of default SSIDs and easily associated beacon signals during the Wi-Fi survey. These included GDWAP1 from an unencrypted access point at the headquarters of General Dynamics Corp. in Falls Church; NASA: Official Use Only from an access point at NASA headquarters on Independence Avenue in Washington; and CMC from an access point located at the house of the

Wireless Vulnerabilities

Security experts warn that wireless communications have certain vulnerabilities that need to be addressed. Among those threats:

Rogues: These are cheap ($100 or less) consumer-grade access points, most likely unauthorized, that have the potential of opening up an enterprise network to anyone within the range of the rogue access point. Users frustrated by lack of wireless access, easy installation and a continuing drop in the cost of access points make this a serious threat that will not go away.

Bug lights: The Wi-Fi utility in Microsoft Corp. Windows XP constantly searches for access points like moths headed toward a flame. This utility makes it easy for a hacker to set up an access point that XP clients will use. If that client is connected to a wired network, it will serve as a bridge for intruders.

Automatic address assignment hacks: Many wireless local-area networks use the Dynamic Host Configuration Protocol to assign IP addresses. That means a hacker can obtain an IP address and a connection to the access point and the network behind it as easily as an authorized user.

Man-in-the-middle attacks: Hackers collect IP addresses from access points and client cards during an initial association process and then set up a fake access point that looks like the real one, diverting traffic to the hacker.

Denial-of-service attacks: Like a polite dinner guest waiting his turn, the Wi-Fi Media Access Control layer avoids transmission when it senses other radio frequency activity. Hackers can exploit that vulnerability by flooding an access point with traffic and setting up a high-power radio frequency generator that denies legitimate users access to the network until the denial-of-service attack ends.

Commandant of the Marine Corps at 8th and I streets in Washington.

Trouble on the cheap

Vendors and analysts said the FCW survey illustrates security problems federal agencies and contractors need to face with the rise of Wi-Fi technology during the past four years. Sheung Li, product line manager for Atheros Communications Inc., a Wi-Fi chip manufacturer, estimates there are 50 million active Wi-Fi devices nationwide. Abner Germanow, an analyst with International Data Corp., a research firm based in Framingham, MA, said worldwide shipments of Wi-Fi devices could hit 19.2 million units in 2004, up from 11.3 million units in 2003.

Wi-Fi's market growth has led to a steep drop in prices for access points, with consumer access points from companies such as the Linksys division of Cisco selling for $40 through Internet retailers. Linksys access points feature plug-and-play capabilities, taking less than a minute to set up.

The combination of low cost and easy installation facilitates rogue access points, which is a serious concern for agency and defense contractor officials, said Richard Rushing, chief security officer of AirDefense Inc., a Wi-Fi security company based in Alpharetta, GA, that sells stand-alone and networked Wi-Fi sensing systems. Rogue access points have the potential to open enterprise networks to sniffing by potentially malicious adversaries and contractors. Federal agencies need to have an active program to detect and prevent rogue access points. Steinbach said CSC officials have a policy barring installation of unauthorized access points, and they could fire any employee who installs one. Steinbach said the rogues discovered by FCW have been disconnected and emphasized that any intruder attempting to use them to penetrate CSC networks would have been stopped by firewalls on the company's wired networks. "We have multiple layers of security," Steinbach said. He added that CSC has contracted with AirDefense to provide systems with around-the-clock monitoring capabilities immediately. ■

About the Authors

Bob Brewin and Frank Tiboni are editors with FCW.com, an electronic news publication produced by FCW Media Group. Contact at *www.fcw.com*

Department of Homeland Security Announces Over $2.5 Billion in Grants

Secretary of Homeland Security Tom Ridge recently announced the recipients of $1.66 billion in grants to states and an additional $855 million in grants to urban areas to fund first responders and support state and local resources necessary to prevent, respond and recover from acts of terrorism and other disasters. Totaling over $2.5 billion in direct assistance to state and local governments for their preparedness and planning needs, these funds augment the nearly $9 billion already delivered to state and local governments and first responders since the creation of the Department of Homeland Security.

"This funding enhances the preparedness of the entire nation while targeting resources where they are needed most," said Secretary Ridge. "We have implemented a national strategy for homeland security that includes shared responsibility and accountability in equipping our front-line first responders with the resources they need to protect our citizens. The continuing maturation of our grants programs, streamlined distribution process and greater accountability measures will ensure that, with this new allocation of over $2.5 billion, we are even better enhancing the capabilities of our nation's first responders to prevent terrorism and respond to emergencies. State and local jurisdictions can expect even more support in the coming months, as we announce further awards in port security, mass transit security and assistance to fire fighters."

Under the state Homeland Security Grant Program, each state, territory and the District of Columbia receives a portion of the $1.66 billion in grants based on a formula consisting of a baseline amount plus the population of the state or territory. The funding is used for equipment, training, planning and exercises. The Urban Area Security Initiative (UASI) provides additional resources to those areas with greater security needs by allocating $855 million in a formula that considers a number of factors including population and population density; critical infrastructure; threat information; formal mutual aid cooperation; and law enforcement investigations and enforcement activity.

The recipients of this round of FY'05 Homeland Security grants will benefit from new measures recently adopted following recommendations from a task force convened by Secretary Ridge to expedite the flow of funds. State and local governments may now have up to 120 days to draw down funds in advance of purchase and investments, as compared to the three to five days allowed previously, so that even small localities have the buying power to purchase expensive or backordered equipment. The Department of Homeland Security also has hosted training seminars and coordination calls with states and urban areas to ensure that they are coordinating to prevent delays in the funding flow. Combined with a

streamlined online application process, these statutory and educational measures will help Homeland Security funds flow as fast as possible to the hands that need them.

The Department of Homeland Security is ensuring that taxpayer dollars are being used to meet the real security goals and objectives identified by the states. All 56 states and territories and the UASI areas have conducted risk, capability, and needs assessments, and have developed multi-year homeland security strategies as a condition of grant awards. The department maintains oversight controls with onsite monitoring of all states, territories and UASI areas, and our reporting requirements provide additional oversight to ensure that states and localities spend their grants for the homeland security priorities identified in their strategies.

"With these new grants, the Department of Homeland Security is building upon nearly $9 billion already allocated to equip, train and prepare our first responders and local law enforcement to prevent incidents and to be ready should one occur," said C. Suzanne Mencer, Executive Director of State and Local Government Coordination and Preparedness. "I have visited states and communities and observed restored emergency operations centers, sophisticated equipment, multi-discipline exercises and new networks of communication and planning. I am inspired by the efforts conducted by these homeland security professionals across the country. This new round of grants will enhance the work already underway and address the new priorities the department and our state and local partners continue to identify."
www.dhs.gov

EVENTS CALENDAR

January 2005

10-12: Implementing Business Continuity From Strategy To Reality
Singapore
Web: http://www.bcpasia.com

8-22: World Conference on Disaster Reduction
Kobe, Japan
Web: http://www.unisdr.org/eng/wcdr/First-Announcement-WCDR-eng.pdf

20-21: Business Continuity Management Workshop Series
Hong Kong
Web: http://www.bcpasia.com

21-22: Enterprise Digital Rights Conference
San Francisco,CA
Web: www.acius.net

February 2005

7-11: Physical Security: Introductory Applications & Technology
Washington, DC
Web: www.asisonline.org

9-11: Sixth Annual Aviation Security Summit and Exposition
Las Vegas, NV
Web: http://www.worldrg.com/AW500/index.html

1-2: Introduction to Computer and Network Security
Dallas, TX
Web: www.gocsi.com/training

3-4: How to Create and Sustain a Quality Security Awareness Program
Dallas, TX
Web: www.gocsi.com/training

8-9: Facilitated Risk Analysis for Business and Security
Seattle, WA
Web: www.gocsi.com/training

10-11: Introduction to End-to-End Digital Investigation
Seattle, WA
Web: www.gocsi.com/training

15-16: How to Perform A Technical Network Vulnerability Assessment
San Diego, CA
Web: www.gocsi.com/training

17-18: A Survey of Computer Forensics Tools and How to Make them Work for You
San Diego, CA
Web: www.gocsi.com/training

March 2005

1-2: EPICC 10th Annual Planning Forum
Burnaby, British Columbia, Canada
Web: www.epicc.org

4: 7th Annual Business Emergency Planning Association (BEPA) Conference & Exhibition
Cleveland, OH
Web: www.redcross-cleveland.org

7: CIO Perspectives: Convergence
UCLA, Los Angeles, CA
Web: www.cio-conference.ucla.edu

10-12: IFMA Management Summit 2005
Orlando, FL
Web: www.ifma.org

22-23: 2005 Business Continuity & Corporate Security Show & Conference
New York, NY
Web: www.flaggmgmt.com/bc

April 2005

4-6: InfoSec World Conference & Expo 2005
Orlando, FL
Web: http://www.misti.com/infosecworld

20-22: Enterprise Wide Risk Management Australia 2005
Sydney, Australia.
Web: http://www.terrap-inn.com/2005/EWRM_AU/

24-27: ESS 2005 Annual International Users Conference
Phoenix, AZ
Web: www.essexpo.com

May 2005

11-12: Security Mexico Conference & Expo
Mexico City, MX
Web: www.ejkevents.com

15-18: Fifth Annual Disaster Resistant California Conference
Sacramento, CA
Web: www.sjsu.edu/cdm/drc05

24-26: CPM 2005 West
Las Vegas, NV
Web: www.contingencyplanningexpo.com

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: http://www.cyberinformatics.org/rmci05/

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 regular price 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 908 788-3782

www.ContingencyPlanning.com

Priority Code: 05GA01

❒ My check for $195, payable to Witter Publishing Corp., is enclosed.

Charge $149 to my:
❒ VISA ❒ MasterCard ❒ American Express

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)