

**BUSINESS SURVIVAL<sup>™</sup>**  
A Business Continuity Newsletter for Decision-makers from  
**ROTHSTEIN ASSOCIATES INC.**

*Volume 9, Issue 2*

*Copyright 2007, Rothstein Associates Inc.*

**CONTENTS**

- Business Continuity and Risk Management Are Intertwined, By Julia Graham
- The Strategic Service Level Agreement - Part 1, by Andrew Hiles
- Survey Says: UK Companies Getting Better at Business Continuity Management
- Survey Says: Third Annual Information Security Workforce Study Results
- News
  - Business Continuity Institute Good Practice Guidelines 2007
  - New FEMA Boss Outlines Vision for Agency
  - Gartner: Half of Data Centers Will Have Insufficient Power and Cooling by 2008
  - New National Symbol for Emergency Management
  - NEMA Report: Emergency Management Agencies Focused on Standards
- Events
- Recommended Reading

---

**BUSINESS CONTINUITY AND RISK MANAGEMENT ARE INTERTWINED**  
By Julia Graham, FBCI

The essence of risk management is to understand all the risks inherent in an organization, and then to take the measures necessary to address them in a proportionate manner. The disruption of a business is arguably one of the most significant risks, and permeates virtually every other risk in an organization's risk profile.

I am concerned that some people maintain, despite the evidence, that business continuity management (BCM) and risk management are best treated as separate disciplines and managed by teams working in separate line management silos. How can this be?

For example, failure to produce an adequate BC plan will have an impact on corporate governance risk. Failure of continuity, especially of production, has obvious implications for reputation risk: not to mention operational risk, financial risk and many others too numerous to mention here.

Let's consider a deceptively simple question: Do you source components from more than one supplier, thereby putting up production costs? Or do you just go to one supplier, so adding to the risk BC failure? Your answer will affect the entire organization and should not be reached in isolation.

This is one small illustration of how BCM and risk management are strategic functions that should be taken together at board level.

BCM, in my view, must overlay the risk management framework as a key management and control mechanism and dovetail into every aspect of risk an organization might need to manage. Only once an organization has analyzed its business and understood its risks can it design and implement an effective approach to BCM.

This said, there is a light at the end of the tunnel. Recent and significant strides forward in the recognition of this relationship have been made. The recently published British Standards Institution (BSi) Business Continuity Management code of practice, BS25999, considers BCM as "...complementary to a risk management framework that sets out to understand the risks to operations or business, and the consequences of those risks."

Through BCM, an organization can recognize what needs to be done before an incident occurs to protect its people, premises, technology, information, supply chain, stakeholders and reputation. With that recognition, the organization can then take a realistic view on the responses that are likely to be needed as and when a disruption occurs, so that it can be confident that it will manage through any consequences without unacceptable delay in delivering its products or services. An organization with appropriate BCM measures in place might be able to take advantage of opportunities which have a high risk. Sound familiar? Sounds like risk management to me.

Individuals and organizations will have their own language and interpretations, but this is healthy. However, business continuity and risk management are intertwined; do not try to separate them.

---

*Julia Graham is deputy chairperson of the Association of Insurance and Risk Managers (AIRMIC). The book she recently co-authored with David Kaye, [A Risk Management Approach to Business Continuity](#) is published by Rothstein Associates. Graham is a former member of the Board of the Business Continuity Institute.*

---

## THE STRATEGIC SERVICE LEVEL AGREEMENT - PART 1 by Andrew Hiles, FBCI

*Editor's Note:*

*This is Part 1 of a two-part series on strategic service level agreements.*

There is an alternative to the Balanced Scorecard to align *Information and Communications Technology* (ICT) with business mission achievement: it can be done by the strategic use of **Service Level Agreements** (SLA) — an approach we have been advocating for over ten years.

First, define the mission. Take, as an example, a multinational company – call it Klenehost – selling miniature packs of soap, shampoo, hair conditioner and shower gel to the hotel industry. These are packaged in different ways and customized for specific hotel chains.

Klenehost states: "*Our mission is to be the number one vendor, world-wide, of in-room hygiene products to the hotel industry.*"

Fine - but what does that mean? Number one in what way? The biggest (by annual revenue)? The most profitable? Having seven of the top ten hotel groups as customers? Having a dominant market share in each of the geographic regions in which Klenehost operates? Having the products most liked by hotel guests?

Following Board-level discussion and business analysis, *Critical Success Factors* (CSFs) are developed to reflect the Board's definition of mission achievement. High-level *Key Performance Indicators* (KPIs) are established — these are the numbers and ratios that reflect whether the CSFs have been met. Examples of KPIs could be: return on investment; net profit; turnover; customer

satisfaction ratings from hotel guests; return per employee, market share by geographic region; key account penetration; customer churn rates, and employee satisfaction.

Initiatives can then be undertaken to put the necessary products, infrastructure, tools, methods, research, etc. in place so that mission may be achieved. Capacity plans and Human Resources policies can be put in place to support mission delivery. Service specifications can be developed to ensure that services meet customer and business needs.

However, the problem with KPIs is that they are usually lagging indicators: you may only know whether you have hit the numbers when it is too late to take action to correct under-performance. The KPIs therefore have to be broken down into lower-level business performance requirements and technical performance measurements. Enter **Service Level Agreements**.

In the past, SLAs for information and communications technology were written in technical terms, typically reporting to end users in terms of the platforms from which services were provided. They reported on items such as mainframe, server or LAN availability and response, typically with minimal business content. SLAs tended to reflect technical measurement over which the end user had no control and in which they had little interest. The similarity is with in-flight information provided to passengers. Because the information is available, the passenger is informed of the outside temperature. What use is this information to the passenger? What are they supposed to do about it?

Technical measurement is important, but only to the technicians who can use it to adjust the service to ensure it does meet SLAs and hence support business achievement of KPIs and ultimately of CSFs and mission achievement. Thus the technical measurement is a leading indicator for ICT.

However, technical achievement needs to be put into a business context and the business or support unit needs to have ICT performance reported not on a technical platform level but in terms of overall service quality across all platforms supporting the business activity. The CFO may use PCs, LAN, servers, printers, WAN and mainframe — but these are just tools. As far as the CFO is concerned, the deliverable is what matters, not the tool. Are invoices issued on time? Are credit control systems working effectively? Are debtors chased promptly? Is the payroll out on time? Is the call center working at optimum effectiveness in handling the maximum number of calls, maximizing sales and minimizing customer churn? The ICT technical performance measures need to be translated into business terms, since they then reflect whether or not ICT's customers - the business or support units - are meeting their service levels and hence their KPIs. Timely production of business performance reports enables ICT's customers to take any remedial action necessary to ensure each unit is on course to support overall mission achievement.

---

**Andrew Hiles** is President of Kingswell International, a consulting company specializing in business risk management and service management. He is the author of [The Complete Guide to IT Service Level Agreements: Matching Service Quality to Business Needs](#); [Service Level Agreements: Winning a Competitive Edge for Supply and Support Services](#); [Service Level Agreement Framework on CD-ROM for IT and Technology](#) and [E-Business Service Level Agreements: Strategies For Service Providers & E-Business Professionals](#). All are published by Rothstein Associates Inc.

---

## SURVEY SAYS:

### UK COMPANIES GETTING BETTER AT BUSINESS CONTINUITY MANAGEMENT

According to the latest British Standards Institution (BSI) Business Barometer, the majority of UK companies now take business continuity seriously. A survey conducted for the Business Barometer found that 61 percent of businesses 'recognize the business benefits of business continuity management in terms of reducing risk, satisfying customer requirements, remaining competitive and winning new business.'

Other findings included:

- 80 percent of FTSE 250 companies would expect to last up to a week before feeling serious detrimental effects of a disruption or disaster;
- Just under half (45 percent) have comprehensive supply chain failure plans (18 percent in the 2005 Business Barometer);
- 41 percent are fully prepared for forced business relocation (15 percent in 2005);
- Over half (51 percent) are very well prepared for IT systems failure (27 percent in 2005);
- 46 percent of businesses are required by customers to show they have business continuity measures in place, three quarters now ask their own suppliers to do the same; and
- 40 percent of businesses who are already committed to applying British Standards agree strongly that compliance with the new business continuity standard (BS 25999) is likely to play an important role in staying competitive and winning new business in future. This is compared with only 26 percent of businesses overall.

[www.bsi-global.com/british\\_standards](http://www.bsi-global.com/british_standards)

Source: [\*Continuity Central\*](#)

---

## SURVEY SAYS:

### THIRD ANNUAL INFORMATION SECURITY WORKFORCE STUDY RESULTS

The International Information Systems Security Certification Consortium (ISC)<sup>2</sup>, headquartered in Vienna, Virginia, USA, recently published the results of its third annual Global Information Security Workforce Study, conducted by analyst firm IDC on behalf of (ISC)<sup>2</sup>. According to more than 4,000 information security professionals in more than 100 countries in the largest study of its kind, the most important elements in effectively securing their organization's infrastructure are (in order of importance):

1. Management support of security policies
2. Users following security policy
3. Qualified security staff
4. Software solutions
5. Hardware solutions.

According to the study authors, the top three success factors highlighted the need for public and private entities to focus more time and attention on policies, processes and people, all areas which have been traditionally overlooked in favor of trusting hardware and software to solve security problems. Survey respondents said that firms are now beginning to recognize that technology is an enabler, not the solution, for implementing and executing a sound security strategy.

The study also found that responsibility for executing a sound security strategy is being increasingly shared across organizations, making C-level officers accountable as part of a well-defined and articulated risk management program.

Continuing a trend identified in last year's study, responsibility for securing information assets is shifting from the chief information officer (CIO) into other areas of senior management and business, including chief executive officer, chief financial officer, chief risk officer and chief information security officer, as well as legal and compliance departments.

"For organizations to proactively secure and protect their infrastructure, information, financial and physical assets requires the unconditional commitment to security at the financial, management and operational levels," said Allan Carey, program manager at IDC who led the study. "Security management will always require the proper balance between people, policies, processes and technology to effectively mitigate the risks associated with today's digitally connected business environment."

IDC analyzed responses from 4,016 full-time information security professionals in more than 100 countries, with nearly 40 percent employed by firms with \$1 billion or more in annual revenue. Respondents came from three major regions of the world: North, Central and South America (57.3 percent), EMEA (Europe, Middle East, Africa) (22.8 percent) and A-P (Asia-Pacific, including Japan) (19.5 percent), and represented firms of various sizes from both the public and private sectors, different vertical industries, and varying core competencies and skill sets. Respondents typically had purchasing, hiring and/or management responsibilities.

Other highlights from the 2006 study included:

- IDC estimated the number of information security professionals worldwide in 2006 at 1.5 million, an 8.1 percent increase over 2005. This figure is expected to increase to slightly more than 2 million by 2010, displaying a compound annual growth rate (CAGR) of 7.8 percent from 2005 to 2010. As a comparison, the projected growth in the number of IT employees globally in the same timeframe is 4.6 percent.
- Common security technologies being implemented by companies across all regions were biometrics, wireless security, intrusion prevention and forensics tools. Biometrics ranked either number 1 or 2 across all regions.
- Information security risk management has risen to the top as a training priority in both the Americas and EMEA and is No. 2 in Asia Pacific. This will continue for the foreseeable future as organizations struggle to gain control over their risk posture, develop a flexible framework to quickly adapt to new environmental factors, and provide visibility into their greatest risks.
- Overall, organizations were spending a greater percentage of their information security budgets on personnel and training in 2006 than in 2005. They spent more than 41 percent of their security budgets, on average, on personnel and training to staff projects and support post-deployment management.

To download a copy of the study, see [www.isc2.org/workforcestudy](http://www.isc2.org/workforcestudy).

Source: [Continuity Central](#)

---

## NEWS

### Business Continuity Institute Good Practice Guidelines 2007

The BCI published the first Good Practice Guidelines in 2002. GPG05 was issued following an extensive rewrite to take into account the latest thinking in BCM internationally and to recognize increasing maturity in BCM practice across all sectors, public and private.

This 2007 guide to implementation of best practice in Business Continuity Management (BCM) has been prepared to support the launch of **BS 25999-1: A Code of Practice for Business Continuity Management** by the British Standards Institution. It can be viewed as an implementation guide to BS25999 and as a definitive text for those wishing to understand BCM principles and practices in a more comprehensive manner.

The Good Practice Guidelines provide an overview and guidance on good practice covering the whole Business Continuity Management (BCM) Lifecycle from the initial recognition of the need for the development of the program to the on-going maintenance of a mature Business Continuity capability.

Download GPG 2007 at <http://www.thebci.org/gpg.htm>.

---

### New FEMA Boss Outlines Vision for Agency

The Federal Emergency Management Agency's (<http://www.fema.gov>) new director, R. David Paulison, recently spelled out his vision for the embattled agency at the National Press Club.

"I want FEMA to be the preeminent emergency management agency for the Nation," said Paulison. "Why? Because FEMA must regain the confidence of the American people and set the standard for best practices in emergency management."

"How are we setting about accomplishing this?" he continued. "For the past year, we have concentrated on improving our operational core competencies, in such areas as: incident management, operational planning, disaster logistics, emergency communications, customer service to disaster victims, and public communication.

"The 2005 Hurricane Season challenged this nation and FEMA as never before. It was a wake-up call for all of us. We learned significant lessons in 2005:

- Communication – information sharing – was probably the single largest failure at the local, state and federal level.
- Logistics – knowing where supplies are and having the ability to deliver them to the right place, at the right time, and in the right quantity.

- Disaster assistance to victims – getting identities verified and registered to expedite the delivery of aid.

"We've taken significant steps to address these problems. In the area of communications and situational awareness – one of the clearest lessons was the fact that a unified command is essential in responding to disasters. Real-time information sharing is occurring at all levels including local, state and federal. Everyone is being kept informed through a Common Operational Picture. Federal Incident Response Support Teams – or FIRST Teams – are at the ready to deploy and provide situational awareness of disasters. Advances in technology are being utilized – Satellite imagery, upgraded radios and frequency management are the new standard. All these actions are being planned in advance – so that the agency is ready on Day One for any disaster.

"We are also beginning to concentrate efforts on improving our business processes to create more robust systems, and to develop best-in-class capabilities, we have begun a series of agency-wide organizational assessments in areas that range from human resources and logistics to budgeting, communications, financial management, procurement and data systems management. The findings from these assessments will provide a solid baseline of where we are today, and a clear direction of the actions we will need to take to reach our vision. We are developing a results-oriented culture that is focused on delivering best-in-class service.

"But there is much to do beyond the confines of one agency. We will also need to learn how to work together better within the larger emergency management community. As we strengthen FEMA and align with this vision, what can America expect of us? America can expect that we will:

- Instill public confidence that FEMA is an agency that works for all of our citizens.
- Capitalize on partnerships among the local, state and federal authorities-because we will bring value.
- Manage our assets more efficiently and effectively.
- Help the Nation continue to build a culture of preparedness.
- Develop international protocols for emergency management, so we can be more effective when we are called upon to help others around the world.
- Be better able to marshal effective national responses to disasters.

"FEMA's challenges are great, but so is our determination to meet and exceed the expectations of the American public. The men and women that make up FEMA are dedicated to strengthening the Nation's preparedness and our ability to respond and recover from disasters."

Source: FEMA, [www.fema.gov](http://www.fema.gov)

---

## Gartner: Half of Data Centers Will Have Insufficient Power and Cooling by 2008

Organizations are increasingly deploying more computing power, but, by 2008, fifty percent of current data centers will have insufficient power and cooling capacity to meet the demands of high-density

equipment, according to Gartner, Inc. (Stamford, CT). Gartner analysts discussed new solutions in power and cooling management at the recent Gartner 25th Annual Data Center Conference.

"With the advent of high density computer equipment such as blade servers, many data centers have maxed out their power and cooling capacity," said Michael A. Bell, research vice president for Gartner. "It's now possible to pack racks with equipment requiring 30,000 watts per rack or more in connected load. This compares to only 2,000-3,000 watts per rack a few years ago."

"Increased power translates into significant increase in heat gain, where the electrical cost to cool the data center can equal or exceed the power to energize the computer equipment," Bell said. "The heat produced by this high density requires new solutions in power and cooling management, specialty cooling solutions, data center design and layout, and processor efficiency."

Traditionally the power required for non-IT equipment in the data center (for example, cooling, fans and pumps) represented about 60 percent of total annual energy consumption. As power requirements continue to grow, energy costs will emerge as the second highest operating cost in 70 percent of worldwide data center facilities by 2009. However, a flurry of innovation is under way that will converge during the next three years to substantially mitigate the power/cooling issue.

"Equipment manufacturers are developing more energy-efficient enclosures, processors and cooling solutions," Bell said. "The leading processor manufacturers are battling to produce more energy efficient chipsets. Server manufacturers are employing more-efficient power supplies, heat sinks and power management systems, as well as offering a host of in-rack cooling solutions, supplemented by facility design and assessment services. We'll see fully integrated management systems that will monitor and manager server workloads and power/cooling demand and optimize capacities in real time."

To build an optimized, reliable and efficient facilities environment, Gartner recommends that data center managers take a holistic approach in planning, designing and laying out the data center to optimize power and cooling capacity. This should include looking at all the variables from site location to building type, building systems, rack configuration, equipment deployment, and airflow dynamics must be integrated and optimized.

[www.gartner.com/us/datacenter](http://www.gartner.com/us/datacenter)

---

## New National Symbol for Emergency Management

Recently, the International Association of Emergency Managers (IAEM) and the National Emergency Management Association (NEMA) unveiled a new national symbol to promote Emergency Management and to help Americans understand how and why it is so important to their lives, and to inspire people to become more involved in their own protection and preparedness. The new logo was unveiled in Washington, D.C., by FEMA Director David Paulison, DHS Undersecretary George Foresman, NEMA President Albert Ashwood, and IAEM President Mike Selves.



The symbol's three stars remind the public that local, state and Federal levels are all vital in preparing for and responding to emergencies. "One of the biggest challenges emergency managers face, as a profession, is dispelling the misconception that our function is simply the sum total of the efforts and resources of the emergency services," stated IAEM President Mike Selves. "The public can identify with firefighters, police and EMTs. However, the idea that there is a profession of public administration, called Emergency Management, whose job is to facilitate the creation of basic disaster policy framework and to coordinate the implementation of the policy during a disaster, is not well understood. Our job ties together not only the responders but also the decision makers, public and private agencies not normally associated with emergency response and a whole array of other elements of the local community before, during and after any disaster event."

[www.iaem.com](http://www.iaem.com), [www.nemaweb.org](http://www.nemaweb.org)

---

## **NEMA Report: Emergency Management Agencies Focused on Standards**

Released late in 2006, the 2006 Biennial Report from the National Emergency Management Association (NEMA) reveals ever-increasing responsibilities for state emergency management agencies; an ongoing struggle for adequate federal funding; and states leading the way in continuous improvement for their emergency management programs.

While all states have homeland security functions, most are tasking significant homeland security responsibilities to their state emergency management agencies. Three national priorities identified by the U.S. Department of Homeland Security – the National Response Plan, the National Incident Management System and the National Preparedness Goal – are assigned most frequently to emergency management for implementation. The same is true for risk and vulnerability assessments, where emergency management takes the lead in eighteen states.

Unfortunately, these growing responsibilities that are mandated by the federal government are not supported by adequate funding. The Emergency Management Performance Grant is the only federal funding available to state and local governments for all-hazards planning, training and exercises as well as some personnel costs. The report says that now there is an estimated \$287 million shortfall in the program. This is up from an earlier estimated shortfall of \$260 million. The fear is that as the gap grows, the nation's ability to respond to disasters of all types is seriously compromised.

The report also reveals some worrisome trends. Beginning in fiscal year 2003, Congress reduced the funding formula for state hazard mitigation – activities that help reduce the devastation caused by future disasters – from 15 percent to 7.5 percent of disaster costs. While recent reform legislation eliminated the 7.5 percent restriction, the cap forced states to either reduce the amount they spent on critically needed mitigation programs; suspend buy-out assistance programs for flooded communities; or eliminate projects all together.

According to the report, as mitigation spending went down, response and recovery expenditures went up. In 1999 for example, when mitigation spending totaled \$498 million, response and recovery was at \$672 million. Four years later, mitigation spending fell to \$310 million, but response and recovery spending had increased to \$746 million. The cycle continued in 2005 when mitigation spending decreased again, this time to \$122 million. Response and recovery spending went up to \$794 million.

Among the positive findings were that an overwhelming majority of states - 46 – are making use of established standards to assess capabilities and address shortfalls in their state emergency management programs. Eleven states are taking it even further, requiring local jurisdictions to use standards, such as those in the Emergency Management Accreditation Program, in the development of annual work plans. This trend of using standards could have far-reaching implications. Regardless of their size or scope, all disasters start as local events. Standards would result in a more comprehensive emergency management program at the local level, which would mean greater capability when a disaster occurs.

Finally, the report shows that the mutual aid system in the U.S. continues to strengthen. The Emergency Management Assistance Compact, a national mutual aid agreement that allows support across state lines when a disaster occurs, played a key role in the Hurricanes Katrina and Rita response. By spring 2006, the compact had deployed nearly 66,000 people from 48 states, at a cost of more than \$830 million. The full report is available for purchase on the NEMA Web site, [www.nemaweb.org](http://www.nemaweb.org)

Source: NEMA

---

## EVENTS

### February 2007

19-22: **Enterprise Risk Management Africa 2007**; Johannesburg, South Africa

<http://www.terrapinn.com/2007/ERMZA/>

### March 2007

16: **Disaster Preparedness Summit**; Kansas City, MO

[www.disasterpreparednesssummit.org](http://www.disasterpreparednesssummit.org)

19-21: **Disaster Management 2007 Exhibition & Conference**; New Delhi, India

<http://www.servintonline.com/dm2007/index.htm>

20-21: **2007 Business Continuity & Corporate Security Conference and Exposition**; New York, NY

<http://www.flagmgmt.com/bc>

22: **Disaster Preparedness Summit**; Philadelphia, Pennsylvania, USA

[www.disasterpreparednesssummit.org](http://www.disasterpreparednesssummit.org)

25-28: **Spring World 2007 (Disaster Recovery Journal)**; Orlando, Florida, USA

[www.drj.com](http://www.drj.com)

26-30: **Business Continuity Awareness Week – Europe**

[www.thebci.org/bcaw.htm](http://www.thebci.org/bcaw.htm)

**April 2007**

12: **Disaster Preparedness Summit**; Houston, Texas, USA

[www.disasterpreparednesssummit.org](http://www.disasterpreparednesssummit.org)

23-25: **Continuity Insights Management Conference**; New Orleans, Louisiana, USA

[www.continuityinsights.com](http://www.continuityinsights.com)

24-25: **DRI Asia 2007**; Singapore

<http://www.driasia.org/>

30-May 3: **Disaster Forum 2007**; Banff, Alberta, Canada

<http://www.disasterforum.ca/>

**May 2007**

4: **Disaster Preparedness Summit**; New Orleans, Louisiana, USA

[www.disasterpreparednesssummit.org](http://www.disasterpreparednesssummit.org)

7-13: **Business Continuity Awareness Week - Americas and Australasia**

[www.thebci.org/bcaw.htm](http://www.thebci.org/bcaw.htm)

17: **Disaster Preparedness Summit**; Chicago, Illinois, USA

[www.disasterpreparednesssummit.org](http://www.disasterpreparednesssummit.org)

22-24: **CPM 2007 West (Contingency Planning & Management)**; Las Vegas, Nevada, USA

[www.contingencyplanning.com](http://www.contingencyplanning.com)

**June 2007**

12: **NEDRIX Summer Conference**; Nashua, New Hampshire, USA

[www.nedrix.com](http://www.nedrix.com)

**July 2007**

8-11: **17<sup>th</sup> World Conference on Disaster Management**; Toronto, Canada

[www.wcdm.org](http://www.wcdm.org)



## RECOMMENDED READING

*These and hundreds of other books, software tools, videos and research reports are available from **THE ROTHSTEIN CATALOGS ON DISASTER RECOVERY AND SERVICE LEVEL MANAGEMENT** at [www.rothstein.com](http://www.rothstein.com):*

---

### **EMOTIONAL CRISES IN THE WORKPLACE: PROTECTING YOUR BUSINESS' BOTTOM LINE**

By Vali Hawkins Mitchell, Ph.D., LMHC  
Philip Jan Rothstein, FBCI, Editor

The failure to adequately address the victims and the emotional dimensions of corporate problems is what changes adverse events into crises and catastrophes. Buildings can be replaced; machines can be fixed; products can be re-engineered and re-marketed; but leaving the needs of victims unmet, denied, or trivialized, and failing to address the emotional impact of events and behaviors can cause permanent damage and often defines careers.

**Emotional Crises in the Workplace: Protecting Your Business' Bottom Line** is an interesting, comprehensive, and constructive approach to adding this key management ingredient to the manager's role. This book's goal is to arm the individual with enough information and structure to persuade the boss to take a shot at adding this skill and knowledge that will help managers and leaders preempt or at least begin to recognize the signs of corrosive emotional distress.

*2005, Order #BSN771*

---

### **NIMS: INTRODUCTION TO THE NATIONAL INCIDENT MANAGEMENT SYSTEM Video plus Model Procedures Guide by Emergency Film Group**

**NIMS: Introduction to the National Incident Management System** is designed to provide training and information to emergency management, EMS, firefighters, police, personnel at federal agencies, hospital and public health personnel, and others who may be called upon to respond during times of emergency, or who may be involved in managing important events.

The program studies the three basic concepts that form the basis of NIMS, and explains the advantages of using a standardized incident management system during complex response situations. The emphasis is on Command and Management.

Using footage of actual and training events, the program will show how command is established and transferred and the role of emergency operations centers in the incident management system. The concept and use of unified command will be explained, as well as the makeup of the incident commander's staff and the four major sections with roles and responsibilities of each.

*2006, DVD or VHS, 25 minutes plus Model Procedures Guide. Order #BSN790*

---

**THE COMPREHENSIVE BUSINESS CONTINUITY MANAGEMENT PROGRAM: Business Impact Analysis, Business Continuity Plan and Crisis / Risk Management Plan Development Templates on CD-ROM**

by Douglas M. Henderson

**The Comprehensive Business Continuity Management Program** is a complete program for business that includes advice for all development steps from the Information Collection Process, through the Business Analysis, to the actual Business Continuity and Crisis Response documentation and finally with assistance for the ongoing exercising and maintenance process.

**The Comprehensive Business Continuity Management Program** follows professional standards as recommended by the Disaster Recovery Institute International, Business Continuity Institute Good Practices Guide, NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs as well as industry best practices.

*2006, 750+ pages on CD-ROM. Order #BSN789*

---

**ROTHSTEIN ASSOCIATES INC.**

4 Arapaho Rd., Brookfield, CT 06804-3104  
203.740.7400 or 1.888.ROTHSTE~~in~~; fax 203.740.7401  
email: [newsletter@rothstein.com](mailto:newsletter@rothstein.com)  
[www.rothstein.com](http://www.rothstein.com)

Newsletter Editor: Paul F. Kirvan, FBCI  
Executive Editor: Philip Jan Rothstein, FBCI  
Copyright 2007, Rothstein Associates Inc. All Rights Reserved

**BUSINESS SURVIVAL™** is sent *ONLY* by YOUR subscription request!  
**To unsubscribe:** email [newsletter@rothstein.com](mailto:newsletter@rothstein.com), subject "UNSUBSCRIBE-BSN."