THIRD EDITION

THE DEFINITIVE HANDBOOK OF BUSINESS CONTINUITY MANAGEMENT

EDITED BY

ANDREW HILES

Preface

David Honour

David is editor, http://www.continuitycentral.com, the global news, jobs and information portal for the Business Continuity profession.

Since the second edition of *The Definitive Handbook of Business Continuity Management* was published in 2007 the world has gone through a period of major turbulence, with the ‘credit crunch’ leading to a global financial sector crisis and subsequent recession. These events resulted in greater scrutiny of financial sector regulation and calls for better Enterprise Risk Management (ERM). Focus has now turned to how ERM and Business Continuity Management relate to each other and what convergence should be seen between these two disciplines.

The other major global crisis which occurred since 2007 was the declaration in April 2009 that the H1N1 ‘Swine Flu’ virus had reached pandemic status. The previous couple of years had seen much contingency planning in this area, and every Business Continuity Plan worth its salt included pandemic planning provisions. The pandemic declaration saw many of these plans being invoked. In hindsight the linking of plans with the World Health Organization’s pandemic warning levels may have been too prescriptive, resulting in what many saw as overreaction and hype. However, whatever criticism they may have faced, Business Continuity managers shouldn’t lose sight of the fact that the pandemic virus could have been much more virulent. And the next might be. There is no room for complacency where pandemic planning is concerned; and there is no guarantee that it will be twenty years before the next pandemic outbreak.

Other notable events which have raised the profile of Business Continuity Management since 2007 include:

- severe summer and autumnal storms causing major floods across Europe;
- winter snow events causing prolonged disruption in the US, the UK and western Europe;
- powerful earthquakes in Haiti, Chile and China;
- ongoing terrorist attacks linked to Al Qaeda;
- the eruption of an Icelandic volcano, releasing clouds of volcanic ash that closed European airspace for several days.

Within the Business Continuity profession the years since 2007 have been ones of consolidation and evolution rather than dynamic change. Business Continuity standards have been scrutinized and improved and industry-wide tests, notably in the financial sector, have provided lessons for improvement, as well as benchmarking information to enable higher quality Business Continuity Management systems to be developed.

If Business Continuity philosophy has progressed at a relatively stately pace, the technology areas which Business Continuity Management supports have seen major changes. Cloud computing and virtualization present the promise of reduced costs for IT Disaster Recovery as well as providing many opportunities for reducing the costs of implementing high-availability environments. Advances in deduplication and data compression techniques also provide new tools for Disaster Recovery and data protection.

When *The Definitive Handbook of Business Continuity Management* was first published in 1999, Business

Continuity Management was seen as an esoteric novelty, which was only of relevance to the largest of organizations and mainly focused on the recovery of IT systems. Now, in 2010, Business Continuity is truly a mainstream management discipline, taught at universities around the world (often using this book) and represented in senior posts within the vast majority of companies and the public sector, in every corner of the world. It is an indisputable fact that Business Continuity Management has come of age.

Introduction to the 3rd Edition

Andrew Hiles, FBCI – UK
Andrew is a Director of Kingswell International Limited, a global consultancy in all aspects of Business Risk Management.

Introduction

Welcome to what we believe to be the most authoritative work on Business Continuity Planning yet produced.' These were the opening words to the introduction to the first edition of this book, written in 1999. We believe these words were equally true for the second edition, published in 2007, and remain true for this, the third, edition.

Since the second edition of this book, much has changed – and much has not. Threats, whether natural or man-made, abound. Organizations are making the same mistakes: history repeats itself. The world economic order has changed, perhaps for good. Supply chain issues and interdependencies have been highlighted. Virtualization technology and techniques have had a major impact on ICT Disaster Recovery. BC standards and guidelines have spawned and multiplied from the welcome firstborn to an extended family of squawking, confusing and sometimes contradictory – and plain ornery – relatives. We have seen a similar growth in the number of related professional institutes and the number of existing institutes extending their reach into risk and continuity. While acknowledging and reflecting this, we have tried to avoid being partisan, reflecting good practice, whatever its source.

You will notice the book has got heavier! In presenting this third edition, we have retained sound components and solid foundations provided by the first and second editions, which we have thoroughly updated where they have been retained. We have incorporated current thinking on well-established disciplines. In addition, we have sought to broaden the book’s global reach, embracing good practices with contributions from all over the world. We have tried to make it more inclusive, inviting input from the premier league of BC professionals, professional associations and institutes, with some 25 contributors from all round the globe. We have also reflected the increasing acceptance of Business Continuity as an academic discipline by inviting contributions from leading BC academics.

The third edition contains not only updated material, but much completely new material on:

- enterprise management and risk assessment;
- BC and business strategy;
- risk and business impact analysis;
- emergency response and operations;
- BCP development;
- ICT Disaster Recovery including virtualization, cloud computing and data backup;
- BC in the supply chain;
- BC in financial institutions;
- BC for retail;
- BC benchmarking;
- BC-related legislation and standards;
- professional associations, certification standards and resources;
- international BC practices, with country perspectives from India, China, the Middle East and Africa;

- ‘how we did it’ war stories;
- new and updated disaster case studies.

A random snapshot of disasters and developments which have all occurred since the second edition was published in 2007 follows.

Disasters 2008

For four days over the New Year period, Kenya experienced tribal riots resulting in arson that destroyed homes, businesses and farms and left an estimated 300 people dead.

January 28, 2008. China suffered severe snow storms and bad weather. 78 million people were affected: over 800 000 people were evacuated, millions were without power, 600 000 train passengers were stranded and 24 people died. The cost was put at $3.2 billion.

January to April, 2008. A dengue fever outbreak in Brazil infected over 75 000 people and killed at least 80.

February 3, 2008. Some 45 people were killed and about 450 more injured after two earthquakes in the Republic of Congo, measuring 6.0 and 5.0 respectively on the Richter scale.

February 5, 2008. Some 55 people were killed and hundreds more injured after tornadoes hit Tennessee, Arkansas, Kentucky and Alabama.

February 7, 2008. An explosion at an Imperial Sugar Refinery near Savannah, Georgia killed 14 people and injured more.

March 14, 2008. In Georgia, USA, bad weather and tornadoes killed two people and injured over 30. The CNN Center was one of the many commercial businesses hit.

March 17, 2008. Flooding and bad weather affected states from Pennsylvania to Texas causing road closures, evacuations and the deaths of 13 people.

March 19, 2008. The Ulyanovskaya mine, located in the Kemerovo region of Siberia, about 2000 miles east of Moscow, suffered a massive methane explosion nearly 900 feet deep. Rescuers saved 90 miners, leaving 107 dead.

March 22, 2008. A stockpile of old ammunition, stored at a Mozambican army facility in the outskirts of the city of Maputo, blew up. It started fires and killed 117 people.

May 11, 2008. Tornadoes killed 20 people and left many homeless in southern states of the USA.

May 12, 2008. An earthquake measuring 7.9 on the Richter scale killed over 67 000 in China, leaving hundreds of thousands injured. Subsequent floods and landslides killed many more.

June 9, 2008. Central states of the USA experienced record flooding, ten people died, dams were broken and thousands were evacuated.

June 9, 2008. An ageing oil pipeline sprung a leak in North Pyongyang province. Local residents tried to scavenge the fuel, which caught fire and exploded. At least 110 people died.

June 17, 2008. A flood, the worst in 50 years, hit southern China, killing over 60 people and destroying 5.4 million acres of crops.

June 21, 2008. Typhoon Fengshen struck the ferry *Princess of the Stars* in the Philippines, killing most of the 865 passengers and crew.

August 23, 2008. 12 people died, many more were injured and left homeless as Tropical Storm Faye hit Florida and other southern states.

August 28, 2008. The Kosi River in India flooded, killing 75 and leaving millions homeless or living in camps.

August 28, 2008. Over 130 people died and many more were injured when Hurricane Gustav struck the Caribbean.

September 1, 2008. Hurricane Gustav left Cuba and struck the USA, devastating the Gulf Coast and killing some 26 people in Louisiana, Georgia and Mississippi.

September 5, 2008. Tropical Storm Hanna hit Haiti, killing hundreds and injuring thousands.

September 7, 2008. After a hit by a tropical storm a few weeks earlier, Hurricane Ike killed some 60 people in Haiti. Four more were killed in Cuba, and 80% of homes were destroyed on Turks and Caicos Islands.

September 13, 2008. Hurricane Ike caused more deaths, severe flooding, evacuations and power outages in Texas, Louisiana, Kansas, Missouri and Illinois.

October 6, 2008. An earthquake, measuring *6.6* on the Richter scale, destroyed the town of Nura, Kyrgyzstan. 70 people died and hundreds more were injured.

October 29, 2008. A 6.4 magnitude earthquake struck south-western Pakistan, killing at least 170 people and destroying around 15 000 homes.

November 22, 2008. Brazil again experienced severe weather, leaving 19 people dead and destroying over 80 000 homes.

December 11, 2008. New England, USA suffered precipitation of ice and snow during storms. Power was out and a state of emergency was declared.

Disasters 2009 and 2010

Natural disasters

The World Disaster Report (WDR)’s 2009 (June) Disaster Report announced that disaster deaths totalled 242 662. 93% of these deaths were caused by the cyclone in Myanmar and the earthquake in China, both in May 2008. This is only slightly below the 2004 disaster death toll – the year remembered for the Asian Tsunami.

In 2009, the United Nations International Strategy for Disaster Reduction Secretariat (UNISDR) published a number of documents on disaster reduction.[1] The 2009 figures released by the Belgian WHO collaborating Centre for Research on Epidemiology of Disasters (CRED) cover the period from January 1 to November 2009.

- Out of the 245 disasters in 2009, 224 were weather related, accounting for 55 million people out of the 58 million people affected, 7000 out of 8900 of those killed, and US$15 billion out of the US$19 billion in economic damages.
- In 2009, 11 million people were affected by floods, compared to 178 million people in 2007 and 45 million in 2008.

Insurance company Munich Re’s statistics for 2009, published on December 29, 2009, said natural catastrophe losses were far lower in calendar year 2009 than in 2008 due to the absence on the whole of major catastrophes and a very benign North Atlantic hurricane season. However, the total number of destructive natural hazard events was above the long-term average, 850 being recorded in all. Consequently, despite the lack of really disastrous events, there were substantial economic losses of US$50 billion and insured losses amounted to US$22 billion compared with economic losses of US$200 billion and insured losses of US$50 billion in the previous year.

By way of further comparison, the average number of natural hazard events with relevant losses over the past ten years was approximately 770 per annum. Economic losses came to some US$115 billion on average and insured losses US$36 billion. There were about 75 000 deaths per year due to natural catastrophes on average. Not only the losses but also the death toll from natural catastrophes in 2009 – around 10 000 – were well below average.

Munich Re’s list of the top ten events in terms of fatalities is as follows:

- September-October 2009 (Indonesia): earthquakes, 1195 deaths.
- September 2009 (South East Asia, East Asia): Typhoon Ketsana, 694 deaths.
- October 2009 (China, Philippines, Taiwan): Typhoon Morakot, 614 deaths.
- October 2009 (South East Asia, East Asia): Typhoon Parma, 469 deaths.
- May 2009 (Bangladesh, Bhutan, India): Cyclone Aila, 320 deaths.
- September-October 2009 (India): floods, 300 deaths.
- April 2009 (Italy): earthquakes, 295 deaths.
- September-October 2009 (India): floods, 223 deaths.
- August-September 2009 (West Africa, Central Africa): floods, 215 deaths.
- November 2009 (El Salvador, Nicaragua, Mexico, USA): Hurricane Ida, 204 deaths.

FEMA responded to 59 disasters in 2009, ranging from fires in California, Montana, Hawaii and Arizona; storms and some consequent flooding in Georgia, Kansas, New

York, Arkansas, Louisiana, Nebraska, New Jersey and Alabama; earthquake, tsunami and flooding in American Samoa; through to explosion and fire in Puerto Rico.

Three events triggering losses in excess of $1 billion all occurred in the United States after severe weather and tornadoes hit southern and midwestern regions of the country in February, April and June. The February event triggered the second biggest loss of 2009, with insurance claims totalling around $1.35 billion. The events in April and June caused insured losses of $1.13 billion and $1.05 billion, respectively.

Aon’s *2009 Global Climate and Catastrophe Report* stated that the largest insured losses of 2009 occurred in the US and Europe, but the developing world continued to suffer billions in uninsured economic losses, according to a recently released study.

- According to Aon, Typhoon Morakot that swept through Asia destroyed 3.9 million structures and produced economic losses of over $5 billion, but insured losses only amounted to $100 million.
- Separately, September 30th’s magnitude 7.6 earthquake in West Sumatra damaged or destroyed over 249 800 structures in Indonesia, causing economic losses of $2.2 billion: insured losses were less than 2% of the economic loss total. Indonesian governmental agencies estimated that reconstruction costs would be around $860 million.
- Aon says that Europe and the United States tallied the most insured losses for 2009, primarily due to damaging winter and springtime weather. The largest insured loss of 2008 was Winterstorm Klaus, which hit France and Spain with hurricane-force winds in January 2009, with gusts peaking at 195 km per hour (120 mph), killing 25 people. The storm was the most powerful to hit France

since Windstorm Martin in 1999. It cost an estimated $3.3 billion in insured losses according to Aon and $3.5 billion according to Swiss Re. Elsewhere in Europe, severe hailstorms hit Switzerland, Austria, Poland and the Czech Republic on July 23, causing a total insured loss of $1.25 billion.

- Asia, however, accounted for most of the economic losses of 2009, with flooding and typhoons accounting for the majority of their losses, the report said.

On March 10, 2009 the eruption of the Mount Galeras volcano in Colombia resulted in the evacuation of 8000 people living nearby.

In February 2010, Britain experienced its worst snowstorm since February 1991, disrupting transportation. Over 250 flights were cancelled at Heathrow Airport (London's largest and busiest airport) as it closed its runways, and London's bus and train services were suspended, stranding millions of people (Reuters). The lack of transportation caused nearly *6.4* million employees to miss work, and these disruptions are likely to cost businesses $4.3 billion (Associated Press).

Flood

We have already mentioned floods across the USA and Europe. Amongst other 2009 flooding incidents were:

- January 12 Fiji – 8 dead, 6000 people displaced. Subsequent landslides from January 15 killed 20 and displaced 6000 people.
- January 16, floods in Jakarta, Indonesia, disrupted power supplies.
- February 5, in the Solomon Islands flooding killed at least ten people. Another ten were missing, feared dead.

Torrential rains from January 29 caused widespread flooding and left an estimated 20 000 people homeless and without food, out of a national population of about 550 000 people.

- May 22, Australian authorities declared a natural disaster on Friday and thousands of people were evacuated after days of torrential rain and flooding killed one man and inundated large parts of the country’s east coast. Around 5000 residents in Lismore, in northern New South Wales state, were evacuated from their homes as floodwaters, in some places more than ten metres deep, surged across riverlands stretching along 300 km of coastline.
- July 28, 100-year floods hit Kanata and Stittsville, Canada.
- July, the rains arrived in Zambia earlier than usual, leading to devastating floods. The floodwaters rose and covered the high ground to which the villagers usually retreat, resulting in hunger, disease and the loss of possessions.
- September 27, floods in the Philippines, said to be the worst since 1967, took out information systems and networks.
- November 25, uncommonly heavy rainfall sparked a flash flood in Jeddah, the kingdom of Saudi Arabia’s second largest city. The flood submerged homes and roadways, drowning 120 people and leaving another 40 unaccounted for. Thousands were left homeless and more than 7000 vehicles were destroyed in the city, which has a population estimated at more than three million.
- A report from the Association of British Insurers (ABI) estimated that the floods in Cumbria in the north-

western part of England and parts of southern Scotland in November 2009 exceeded £200 million ($322 million). The ABI reported that insurance claims following the floods were estimated at £206 million ($332 million) and that 60% of this cost related to business damage.

Terrorism

Terrorist activity continued unabated. United States law enforcement agents and partners reported ‘encounters’ with suspected terrorists 55 000 times in the last year; a check against the terrorist watchlist found a match 19 000 times (including multiple hits on the same people), according to testimony presented to the Senate in December 2009.

According to a Time.com posting on December 23, 2009, out of 32 USA domestic terrorist events since 9/11, 12 of them occurred in 2009. Events included an al-Qaeda plot to blow up a train in Penn Station and another plot to blow up a federal building in Springfield. On May 2, 2010, Times Square was evacuated following an attempted car bombing. Faisal Shahzad, a naturalized US citizen, was later arrested.

Wikipedia reports some 282 terrorist attacks worldwide in 2009. While most attacks were in Afghanistan, Iraq and Pakistan, terrorist incidents also took place in Algeria, Canada, Chechnya, China, Colombia, Corsica, France, Greece, Hong Kong, India, Indonesia, Israel, Lebanon, Majorca, Nepal, Norway, Philippines, Somalia, Spain, Sri Lanka, Thailand, Turkey, UK, USA and Yemen.

Fire and explosion

On January 31, 2009 an oil truck overturned in Molo, Kenya, spilling oil. Locals rushed to collect free fuel when the spill ignited, resulting in the deaths of at least 113 people and critical injuries to another 200. The fire came less than a week after a fire in a Nairobi supermarket killed 25. In June, another oil tanker spilled, with four deaths and 25 injuries in an incident similar to that in Molo.

In February 2009, at the end of a major heatwave, bushfires in the state of Victoria, Australia, killed 173 people and injured some 500. The fires destroyed over 2000 homes and deleted whole towns from the map. They were the worst bushfires in Australia’s history and also one of Australia’s worst natural disasters.

From March 31–April 27, 2009 Shell shut down a major crude oil pipeline and several adjoining flow stations in Nigeria’s southern Rivers State following a fire.

On April 17, 2009 there was a major fire at Paarl Print plant in South Africa. The fire at the Dal Josafat Industrial Estate, Paarl, Cape Boland killed 13 employees and contractors and was probably caused by a paper dust explosion.

The July 2009 hailstorms in Switzerland, according to Guy Carpenter, resulted in 150 000 claims totalling more than CHF733 million ($684 million).

Bearing a remarkable resemblance to the 2005 Buncefield fire in the UK (q.v.), from October 23 to October 25, 2009 a fire engulfed the Caribbean Petroleum Corporation refinery and depot in Puerto Rico. The fire destroyed storage tanks containing gasoline, jet fuel and bunker fuel. Flames reached a height of 100 feet (30m) above the refinery. The resulting explosion was measured as a 2.8-magnitude earthquake on the Richter scale and could be heard over five miles away. The tanks exploded at about 00:23 hours and shook windows and doors over two miles away.

In February 2009, the US National Fire Prevention Association presented its overview of fires for 2008:

- 3320 civilians lost their lives as the result of fire;
- 16 705 civilian injuries occurred as the result of fire;
- 118 firefighters were killed while on duty;
- fire killed more Americans than all natural disasters combined;
- 16% of all civilian fire deaths occurred in non-residential property;
- there were an estimated 1.5 million fires in 2008;
- direct property loss due to fire was estimated at $15.5 billion (this figure includes the 2008 California Wildfires with an estimated loss of $1.4 billion);
- an estimated 32 500 intentionally set structure fires resulted in 315 civilian deaths;
- intentionally set structure fires resulted in an estimated $866 million in property damage.

The latest fire statistics for England, published by Communities and Local Government and covering the 12-month period up to March 3, 2009, identified 27 000 fires in non-residential buildings.

In August 2009 a transformer explosion occurred in Siberia at the world's fourth largest hydro-electric plant, destroying three out of ten turbines. Eight people were reported dead, with some 50 missing.

On November 21, 2009 an explosion occurred in the Xinxing coal mine near Hegang in northeast China. 108 people died and 29 more were put in hospital. The explosion happened when 528 people were thought to be in the mine.

On April 20, 2010 an explosion set fire to and subsequently sank the Deepwater Horizon rig, owned and operated by

Transocean and leased to BP, drilling 50 miles (80 kilometres) off the Louisiana coast in the Gulf of Mexico. 11 workers were presumed dead. An estimated 19 000 barrels of oil a day leaked. By the end of June 2010, the value of BP shares had plummeted to less than half their pre-disaster price; losses and clean-up costs could be similar; punitive damages could follow; future deep sea drilling is under threat. In June 2010 BP had to put $20 billion into escrow against claims, forcing the cancellation of its dividend. Law suits are pending. You can outsource the job but not the risks. BP's reputation was only just recovering from disasters in Texas City in 2005; Thunder Horse platform (build problems, 2005–10) in the Gulf of Mexico and leaking pipelines in Prudhoe Bay (2006).

Business Continuity

The Business Continuity Institute (BCI) says that it has estimated that the UK economy is losing £11.1 billion a year, the equivalent to 0.8% of UK GDP, to major disruptions due to lack of Business Continuity Management within UK-based organizations.

In North America, over 52% of organizations that have a BCP have invoked it in the last five years.

According to *Continuity, Insurance and Risk* magazine[2] more clients are using managed IT services for Business Continuity.

A report from ABI Research[3] forecasts that spending on Business Continuity and data Disaster Recovery services will explode in the next five years, growing from $24.3 billion in 2009 to more than $39 billion in 2015.

In June 2010, Public Law PL 110-53, *Implementing Recommendations of the 9/11 Commission Act of 2007*,[4] was published in the USA. This law suggests that risk management, business resilience and BC be implemented by all organizations in accordance with standards. In section 901, *Voluntary Private Sector Preparedness Standards; Voluntary Accreditation and Certification Program for the Private Sector*, and 902, *Responsibilities of the Private Sector Office of the Department*, it sets up an audit structure and credentialing agents. While voluntary, the law has significant implications and opportunities for BC professionals.

Disaster Recovery

Zooming in on Disaster Recovery, Symantec Corp. released the results of its fifth annual Global IT Disaster Recovery survey in July 2009:

- The report claims that 93% of organizations have had to execute their Disaster Recovery Plans and the average cost of implementing DR Plans for each downtime incident is US$287 000. The median cost in Canada is US$496 500. The average budget for Disaster Recovery initiatives worldwide is US$50 million.
- The response within Canada reflected the worldwide results, but percentages were noticeably different in terms of virtualization backup practices. Only 10% of Canadian respondents do not back up data on virtualized systems, compared to 36% worldwide.
- The average time it takes to ‘achieve skeleton operations after an outage’ is three hours. To be fully ‘up and running after an outage,’ the average is four hours.

A recent survey by ITIC/Stratus Technologies said that, although organizations know they need more reliable information systems, 49% have no budget for high-availability technology, 40% do not understand what qualifies as high availability and more than 80% cannot make a business case for it because they do not know the cost of downtime.

The results are summarized as follows:

- 16% stated that 20% to 30% of their applications required the highest level of availability.
- 18% said that 50% to 60% of applications needed the highest level of availability.
- 19% said that 80% of their applications required the highest level of availability.
- 81% indicated that the number of applications needing very high availability has increased over the last three years. Another 17% said it ‘remained the same. ’
- 41% said that their most critical applications needed only 99.0% to 99.9% uptime.
- 29% needed 99.95% to 99.99% of uptime.
- 7% reported that they require continuous uptime.
- 16% said that their companies had no specified availability levels.
- 40% had no current budget to purchase a software availability solution. However, 2% said they would pay $2000 to $4000; 8% said they would spend $4000 to $5000; 3% would spend $5000 to $10 000 and 11% said they would spend $10 000 to $15 000 while 5% were willing to spend ’whatever it takes’ to ensure application availability. 30% were ‘Unsure’.
- 52% reported that virtualization has increased uptime and application availability. 18% of the respondents had not yet deployed virtualization. Among those who had, 82% stated that virtualization had increased application availability and uptime. Just 4% of respondents said virtualization had not shown any improvements in

application availability; 18% said availability remained the same and 8% were ‘Unsure’. The report suggests that these figures will change over the next 12 to 18 months with the spread of virtualization.

- 43% indicated they do not track their SLA achievement and are unable to assess the impact in terms of cost or lost productivity. 28% are able to assess the impact of downtime; almost 11% admitted they could not and another 18% were ‘Unsure’.

It is estimated that most large companies spend between 2% and 4% of their IT budget on Disaster Recovery planning.[5]

In April, 2010, the UK Centre for the Protection of National Infrastructure (CPNI) published a new guide which looks at data centre protection from initial site selection through to design, build and operation.[6]

Resilience Engineering

Over the last few years we have seen the concept of ‘Resilience Engineering’[7] taking hold. Usually, risk management approaches look at things in the rear view mirror – we take past incidents and project from them future probability. We take hindsight and from it expect to produce foresight. Resilience Engineering seeks ways to improve robustness, reliability and flexibility of processes and organizations, continually monitoring and revising risk levels. The result of Resilience Engineering is to develop adaptive organizational operations that can flex in the event of equipment breakdown, production demands or financial or market pressures that happen in real life. Success in Resilience Engineering gives the ability to bend before the wind, rather than break – to anticipate that ‘unknown unknowns’ will happen, to adapt, move on and not to fail.

The ANSI/ASIS SPC.1-2009 American National Standard, *Organizational Resilience: Security, Preparedness and Continuity Management Systems – Requirements with Guidance for Use*, was published as a Dutch National Standard (NEN 7131) by the Netherlands Standardization Institute in January 2010. This follows publication as a Danish National Standard (DS 3001) in September 2009 by Danish Standards.

An interesting resilience benchmarking report was published by Resilient Organizations[8] of New Zealand, providing the results of a study undertaken in the Auckland region, the principles of which are generally applicable.

The implications of Resilience Engineering will be significant for BC professionals. We should be open to the concept and embrace it.

Summary

The only thing we can rely on is uncertainty. Disasters happen each year: some, like floods in the Indian subcontinent, are more predictable than others. But equally, each year crisis and emergency response improves, Business Continuity Plans work and Disaster Recovery capability increases. Each year new concepts in disaster planning, prevention and mitigation are developed. It’s not all bad news.

[1] http://www.unisdr.org/publications/index.php?pid=0&tid=33&rid=0

[2] *Costing it up – the effect of the recession on business continuity technology spend,* by David Adams, July 2009.

[3] http://www.abiresearch.com/research/1004739-Business+Continuity+Disaster+Data+Recovery

[4] http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_public_laws&docid=f:publ053.110

[5] http://en.wikipedia.org/wiki/Disaster_recovery#cite_note-0

[6] http://www.cpni.gov.uk/Docs/viewpoint-data-centre.pdf

[7] *Resilience engineering: concepts and precepts* by Erik Hollnagel, David D. Woods and Nancy Leveson.

[8] http://www.resorgs.org.nz/pubs/Benchmark%20Resilience%20-%20ResOrgs%20Research%20Report.pdf

How to Use this Book

Andrew Hiles
FBCI – UK

This book is divided into the following parts:

Section One provides an executive overview of some of the strategic issues pertinent to Business Continuity planning and management.

Section Two covers Business Continuity Management methodology, including planning for business continuity. It broadly follows the ten core competencies of Business Continuity – the common body of knowledge initially agreed between the Disaster Recovery Institute International (DRII) and the Business Continuity Institute (BCI) that forms the foundation of effective Business Continuity planning and management. Although the BCI has condensed these ten into six, in line with British Standards Institution BS 25999 (the UK standard for Business Continuity Management) the elements of the original ten have been incorporated in them.

Appendix 1 provides case studies. Some of these cases are industry classics; some are more recent. What they all have in common is lessons for us now and in the future. The saddest thing about Business Continuity is that so few organizations learn from other organizations' mistakes and experiences. Please, let us learn from history!

Appendix 2 gives some general guidance on various aspects of Business Continuity Management, some light-hearted – but even they have a serious message.

Appendix 3 has been greatly expanded and developed. It provides a background to professional associations and institutes around the world and outlines their membership and certification standards for Business Continuity practitioners – defining and amplifying the skill sets employed in Section Two. We welcome the contributions from those distinguished institutions that responded to our invitation to provide input. We hope this is the start of a process that will lead to greater rapprochement between BC-related organizations and a move towards joint activity between them, rising above parochialism and, ultimately perhaps, providing a unified, global voice on behalf of the BC community. Appendix 3 also identifies international useful resources.

Appendix 4 expounds on international legislation and standards related to BC and explains the many differing BC practices and environments around the world, with contributions from those who live and practice BC there. For those wishing to investigate these further, we have provided references to more detailed surveys and reports.

The book draws on expertise at the highest level, from practitioners around the globe. We welcome their diversity, and the diversity of styles that they use. Each expert places his or her extensive experience openly and freely at your disposal. This volume carries truly international perspectives across all industries and the public sector.

Since each author is writing from their own experience, each chapter provides a self-contained element of the total fund of BC knowledge. It is inevitable that a degree of replication may take place – this is necessary for each author to put his or her own concepts into the appropriate framework and to present their own perspective as a stand-alone chapter. And whenever two experts are gathered together, you probably get three opinions. This is reflected in those chapters comprising more than one part: in some, the second part may be complementary; in others an alternative view may be offered.

There are many wrong ways of implementing BCM, and only a few variations on right ways. You may notice some differences of approach between the authors: however, if you follow the advice that most seems to match your situation, you are unlikely to fail.

It is not the sort of book that you necessarily read from beginning to end: it is a ‘pick and mix’ selection. We suggest you start with Section One, to put BCM into a strategic corporate risk management context. As you move through each of the disciplines and activities outlined in Section Two, you may wish to pause after each chapter and dip into the complementary guideline notes in Appendix 2 and supporting case studies in Appendix 1.

For those of you who are new to BCM, we hope this will provide a fast track to ease the way and speed you to your goal of protecting your organization. For those of you who are more experienced BC practitioners, we hope that at least this book will consolidate your experience, reassure you and confirm your direction – and maybe show you a few new ideas or provide additional justification for your activities.

The ultimate aim for all of us is to create and embed BC and risk management practices in our (or our clients’) organizations that mean ‘business as usual – no matter what!’

Section One
Achieving and Maintaining Business Continuity: an executive overview

1
Enterprise Risk Management

Andrew Hiles, FBCI – UK & France

Andrew is a Director of Kingswell International Limited, a global consultancy in all aspects of Business Risk Management.

Background

While the concept of Enterprise Risk Management has been around for over 25 years, it was formalized largely as a result of initiatives of the Committee of Sponsoring Organizations (COSO).[1]

COSO was formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting (the Treadway Commission) following a number of cases of fraudulent accounting in corporations.

COSO was founded and is funded by the five main professional accounting associations and institutes in the USA:

- American Accounting Association;
- American Institute of Certified Public Accountants;
- Financial Executives International;
- Institute of Management Accountants;
- Institute of Internal Auditors.

The Treadway Commission recommended that the organizations sponsoring the Commission work together to develop integrated guidance on internal control.

COSO is a voluntary private-sector organization, dedicated to guiding executive management and governance entities toward the establishment of more effective, efficient and ethical business operations on a global basis. It sponsors and disseminates frameworks and guidance based on in-depth research, analysis and best practice.

Events, Risks and Opportunities

The impact of an event may be negative, positive or both. Events with a negative impact represent risk, which can prevent value creation or erode existing value. Events with a positive impact may offset negative impacts or represent opportunities. Opportunities are the possibility that an event will occur and positively affect the achievement of objectives, supporting value creation or preservation. Management channels opportunities back to its strategy or objective-setting processes, formulating plans to seize the opportunities.

> **Enterprise Risk Management: Definition**
>
> Enterprise Risk Management (ERM) is a process, effected by an entity’s Board of Directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

The definition reflects certain fundamental concepts. ERM is:

- a process, ongoing through an entity;
- effected by people at every level of the organization;
- applied in strategy setting;

- applied across the enterprise, at every level and unit, and includes taking an entity-level portfolio view of risk;
- designed to identify potential events that, if they occur, will affect the entity and to manage risk within its risk appetite;
- able to provide reasonable assurance to an entity's management and Board of Directors;
- geared to achievement of objectives in one or more separate but overlapping categories.

The definition is intentionally broad. It captures key concepts fundamental to how companies and other organizations manage risk, providing a basis for application across organizations, industries and sectors. It focuses directly on achievement of objectives established by a particular entity and provides a basis for defining ERM effectiveness.

Expanding on Risk Management

The original COSO framework contains five control components needed to help assure sound business objectives. The control components are:

- Control environment;
- Risk assessment;
- Control activities;
- Information and communication;
- Monitoring.

Headline-grabbing scandals such as Enron, Tyco and Worldcom led to demands for stronger corporate governance and risk management. The result was the