

PREVENT, AND THOU SHALL BE SAVED!

A BCM guide to preparing for the apocalypse... and other disasters in 2012

By Glen Oliver, Technical Writer



It's the final countdown! As the chorus to a famous song goes, few experts believe that the days are finally closing in when life as we know it will cease to exist.

To those of you who have been following, this indeed is what most people refer to as the 2012 Phenomenon – a somewhat accumulation of “doom and gloom” predictions of imminent disasters and tragedies which some believe foreshadow the inevitable end of days.

Understandably, most – upon hearing – will immediately dismiss the idea, while others may in fact run for the hills. Regardless of what demise awaits humanity, however, one thing is for sure – 2012 will be a significant year for business continuity management (BCM).

And so, as we welcome the New Year, we present you with a summary of “things to look out for and look into” as BCM practitioners in the “age of the apocalypse.”

Increasing risks and probability of natural disasters

Consider the volcanic eruptions in Iceland and Congo, the destructive earthquakes that hit Christchurch, eastern Turkey and the East Coast of Tohoku in Japan, as well as the recent flooding in Thailand and one thing becomes clear about natural disasters – their risks, probability and consequences are higher than ever.



All Rights Reserved 2011© BCP Asia
Permission to reprint, republish and/or distribute this material in whole or in part for any other purposes must be obtained from BCP Asia.
For information on obtaining permission, send an e-mail message to the enquiry@bcpasia.com.

In the case of earthquakes, for example, the United States Geological Survey reports that there are a total number of 19,849 occurrences worldwide as of December 1 this year – 2,342 of which measured 5.0 and above in the Richter scale.⁽¹⁾

Though it's true that this data does not prove that there is an increase in its probability or frequency, it is unmistakably apparent that the devastations caused by earthquakes in this day and age are more dramatic. And this is taking into account the extent of the aftermaths of this year's occurrences. But what exactly changed the ratio? It may simply be due to the fact that the population at risk has increased.

According to the State of World Population 2011 report by the United Nations Populations Fund, there are now an estimated number of 7 billion people around the globe.⁽²⁾ Sadly, this could be translated as to having more casualties, fatalities and/or property damages in the event of a natural disaster today.

Also concurrent with the increasing human population is the inevitable change in the environment – meaning continuous rise in carbon pollution, decrease and such. Unfortunately, environmental concerns such as climate change are still being overlooked and somewhat addressed inadequately despite the alarming consequences they bring to communities and businesses. Hence, the Intergovernmental Panel on Climate Change forecasts more intense heat waves, frequent and heavier rainfalls, rising sea levels and other environmental disasters throughout the 21st century.⁽³⁾⁽⁴⁾⁽⁵⁾

All in all, natural disasters today cause fatalities, property damages and financial/asset losses at an extremely alarming measure. In a press release by reinsurance company Munich Re, 2011 is the “highest-ever loss year on record” due to natural disasters – with losses amounting to more than five times higher than the first-half average for the past ten years.⁽⁶⁾ Indeed, these things should serve as a “wake-up call” to everyone because when it comes to natural disasters everyone is at risk.

Supply chain vulnerability revisited

In the final issue of Continuity magazine for 2010, Lyndon Bird – international technical director of the Business Continuity Institute – wrote an article that ranked supply chain vulnerability as the top most important issue that had the most impact on the business continuity industry that year.

A year later, it remains to be true.

Businesses only seem to remember about supply chain risks after disruption or disaster strikes. As a result, many companies with suppliers in Japan immediately got into trouble after a magnitude 9.0 earthquake hit the East Coast of Tohoku last March 11.



The recent flooding in Thailand appears to tell the same story. Considered as a “production hub” by a wide-range of industries, Thailand suffered from major economic drawbacks when severe flooding hit the country early this year – causing massive supply chain disruptions, particularly in the automotive and computer hard-disk drive sectors. ⁽⁷⁾⁽⁸⁾

Although indeed unfortunate, it may be difficult for businesses today to find an excuse for not preparing for such scenarios. Considering that a lot of companies already experienced similar problems from last year’s volcanic eruption in Iceland, supply chain risks should definitely have been considered in today’s business continuity plans.

From a different angle, recent events also highlighted concerns about the effectiveness of today’s supply chain practices.

In an online article, ⁽⁷⁾ BCM experts CEO Patrick Brennan calls for an “immediate change” in today’s supply chain risk management – citing four lessons that should be learned from the recent disaster that hit Japan, which are:

- 1 Don’t apply the 80/20 rule to supply chain disaster preparedness
- 2 Identify supplier factory locations before a crisis hits
- 3 Visibility into supply chain sub-tiers remains a key challenge
- 4 Large crisis events shift market share among competitors

Indeed, moving forward, must indeed accept the fact that supply chain disruptions – just like natural disasters – are inevitable. Though indeed this issue appears to have “less news potential” compared to other “social media-friendly” topics today, supply chain vulnerability is an issue that should be on top of every company’s list of concerns.

Growing dependence on technology poses serious risks

For years now, businesses and governments have been reaping the rewards of a fast-growing and developing cyberworld. Today, most specially, it is the norm for businesses to incorporate gadgets and other technologies such as cloud computing or social networking in their daily functions and operations.

With these advancements in the cyberworld, however, also comes the increase in the rate of risks such as cybercrimes.

In fact, in the World Economic Forum Global Risks 2011 Sixth Edition report, cyber-security issues were mentioned first in the “five risks to watch” list – ahead of weapons of mass destruction. ⁽⁹⁾



Relevantly, in a survey conducted by PricewaterhouseCoopers (PwC), ⁽¹⁰⁾ 34% of 3,877 respondents from 78 countries (who are also senior executives and representatives of different businesses) answered yes when asked if they have experienced economic crime in the last 12 months. According to PwC, this is a 13% increase from their previous survey in 2009.

When it comes to the most common cause of cybercrimes, computer viruses or malware was ranked number one in the Norton Cybercrime Report 2011. ⁽¹¹⁾ In the same report, it was also mentioned that cybercrimes via mobile devices are likely to increase.

Vulnerability to cybercrimes, however, is not the only implication of technology dependency in today's businesses. What these surveys failed to reveal are other concerns such as the possible decrease in employee productivity and the inability of some personnel to perform tasks "manually."

From a BCM perspective, such issues can be addressed simply through effective staff training. Online security may indeed require more time and effort, but businesses can definitely start by accepting the fact that all industries are vulnerable to cybercrimes – perhaps most specifically the finance and communications sectors.

Other risks and thoughts to ponder

Indeed, there may be several other issues out there, such as contagion and riots, which businesses should also look into when preparing their BCM plans for the New Year.

In fact, other issues that were included in the "five risks to watch" list are demographic challenges, resource security, retrenchment from globalisation and – as mentioned earlier – weapons of mass destruction. ⁽⁹⁾ And in that same report, the World Economic Forum (WEF) highlighted that these issues have implications (but not necessarily collectively) on global income, social stability, migration, commodity prices and resources, globalisation and the proliferation of nuclear and biological weapons among others.

Although these are probably risks in a broader sense, businesses may indeed choose to look from a "BCM perspective" to make these data more relevant and useful in developing their business continuity plans today. For example, issues on the proliferation of nuclear weapons can be made relevant by considering the nuclear disaster that recently occurred in Japan – which, as we all know, caused enormous problems to businesses around the world.



Now, putting back the 2012 Phenomenon in context, it would indeed be rational for someone to expect of a catastrophic year ahead considering all of these issues at hand. However, comes to mind a popular quote by author Richard Back, which goes “*The mark of your ignorance is the depth of your belief in injustice and tragedy. What the caterpillar calls the end of the world, the Master calls the butterfly.*”

And this probably means that, at the end of the day, it's just a matter of looking if the “glass is half full or half empty.” Although indeed, we have different opinions about the 2012 Phenomenon or such beliefs, the reality is that tragedies will always be part of human life.

It's true, no one knows exactly when will these things be, but we can always choose to be prepared. And this, perhaps, is exactly where the beauty of BCM as a profession and as an industry lies – that even in the face of uncertainty, we can always count on being ready for anything.

References:

- (1) **United States Geological Survey, 2011.** *Earthquake Facts and Statistics*. [online] Available at: <http://earthquake.usgs.gov/earthquakes/eqarchives/year/eqstats.php>. [Accessed 03 December 2011].
- (2) Information and External Relations Division, 2011. *State of the World Population 2011*. United Nations Population Fund.
- (3) Fiona Harvey, 2011. *Extreme weather will strike as climate change takes hold, IPCC warns*. The Guardian . [online] Available at: <http://www.guardian.co.uk/environment/2011/nov/18/extreme-weather-climate-change-ipcc>. [Accessed 03 December 2011].
- (4) Mindy Lubber, 2011. *IPCC Report Confirms What Businesses Already Know: Extreme Weather & Climate Change Has Economic Impacts*. Forbes. [online] Available at: <http://www.forbes.com/sites/mindylubber/2011/11/23/ipcc-report-confirms-what-businesses-already-know-extreme-weather-climate-change-has-economic-impacts/>. [Accessed 03 December 2011].
- (5) Intergovernmental Panel on Climate Change, 2011. *Special Report Managing the Risks of Extreme Events and Disasters to Advance Climate Change Adaptation (SREX)*. [online] Available at: <http://www.ipcc-wg2.gov/SREX/>. [Accessed 03 December 2011].
- (6) Munich Re, 2011. *Accumulation of very severe natural catastrophes makes 2011 a year of unprecedented losses*. [online] Available at: http://www.munichre.com/en/media_relations/press_releases/2011/2011_07_12_press_release.aspx. [Accessed 03 December 2011].
- (7) Patrick Brennan, 2011. *Lessons Learned from the Japan Earthquake*. Disaster Recovery Journal. [online] Available at: <http://www.drj.com/2011-articles/summer-2011-volume-24-issue-3/lessons-learned-from-the-japan-earthquake.html>. [Accessed 04 December 2011].
- (8) Rodd Zolkos, 2011. *Disasters prompt supply chain risk reconsiderations*. Business Insurance. [online] Available at: <http://www.businessinsurance.com/article/20111120/NEWS06/311209972?tags=>. [Accessed 04 December 2011].
- (9) World Economic Forum, 2011. *Global Risks 2011 Sixth Edition*. World Economic Forum.
- (10) PricewaterhouseCoopers, 2011. *Cybercrime: protecting against the growing threat Global Economic Crime Survey*. PricewaterhouseCoopers.
- (11) Symantec Corporation, 2011. *Norton Cybercrime Report 2011*. [online] Available at: http://www.symantec.com/content/en/sg/home_homeoffice/html/cybercrimereport/. [Accessed 03 December 2011].

