

### WHAT DO YOU DO WHEN TOO MUCH BC IS NOT NEARLY ENOUGH?

#### STRATEGIES TO DEAL WITH THE THREATS POSED BY TERRORISM AND NATURAL DISASTERS

29 OCTOBER 2007

Ladies and gentlemen there have been many thought provoking presentations over the last two days so let's have a two minutes debate with your neighbor. The topic, will global warming continue to manifest itself in floods and violent storms? Cyclones have been getting 50% faster and 50% more frequent in the last 50 years. Now turn to your other neighbor and let's have another two minute debate. Will the Internet allow terrorists unparallel advantage as they butt up against the spread of capitalism throughout the world? Clearly it is appropriate to ask what you do when even with the best resilience that money can buy, what do you do when this is just not enough? Of course we are talking about the D-word and whether you bother doing anything at all about the impacts of terrorist incidents or natural disasters from a BC perspective. We need to quite clearly differentiate between Emergency Response and Business Continuity Planning. Let's get Emergency Response out of the way so we can focus on recovery strategy and determine how much planning is enough.

Corporate Emergency Response, Mass casualty plans, EAP Providers, NEC, Virtual meetings, Call Centre, Loud hailers and Rendezvous, Lost communication procedures, Government security clearances. These are the tools for dealing with mass casualties and employee dislocation. These are also the tools for improving communications and working with governments and law enforcement agencies during such events. Mass casualty plans are now standard as terrorism In particular puts every public gathering place at risk. Responding appropriately in the first 15 minutes with scoop and run tactics is when you will have most impact in saving life. Who here has a mass casualty plan? All companies have Employee Assistance Providers on call, and the best companies have well developed systems for providing peer support or fast buddies to use the Singapore Airlines expression. It is now normal to store the list of nominated emergency contacts for all employees in fire proof safes and to have duplicate copies off site. Who here does that? The best companies continually account for all people on site and are able to do immediate name calls and head counts if evacuating facilities. Who here can account for all employees in 30 minutes of any evacuation, anywhere? Invacuations, staying on site with the air conditioning switch off, is equally important as traditional evacuations when dirty bombs or toxic gas are involved. In high-rise buildings elevators maybe the fastest way out regardless of warnings. Virtual Crisis Team meetings are now the norm as indeed are fully equipped alternate locations and satellite phones. The best companies still resort to old fashioned switchboards in time of crisis through the use of internal Call Centres and hotlines to contact employees. Who here has a permanent employee hot line? Loudhailers are as important as ever in additional to rendezvous points in the absence of sirens to directly alert people to serious incidents. A common point of contact in the event of an emergency is essential as is a community system for lost communications, lost communications procedures for travelers and GPS tracking of assets. Who here has a traveler tracking system that would allow you to locate any employees anywhere in the world in 24 hours? Do you think we need a national emergency readiness standard for business in your country? Should there be a national

liquid fuel ER plan like we have in Australia? Should it be voluntary, or a factor in obtaining terrorism insurance? Do we have any insurance companies in the room? Hands up please? Can we ask you if there national liquid fuel ER plan like we have in Australia in every country? With a show of hands, who here thinks that the risk of terrorist incidents or natural disasters is so remote from their business that that there is no justification for including a contingency plan in the BCP?

What do you do when the Emergency Response is over and you find your self starting from Ground Zero after a natural disaster or terrorist event? Our advice here is to ensure that there is a Crisis Management Team in place. It is still surprising the number of companies that do not have simple plan for their leadership to meet in a primary or secondary location or virtually. Who here can convene their CMT virtually and instantly? Who here is interested in seizing market opportunity? The discipline of Business Continuity has actually been around for a very long time as just plain ordinary contingency planning. Noah probably had the first formal plan with the Ark and his solution to embark one male and one female of every type of animal just before the great flood. Like Noah, another very simple option is to implement some form of succession planning by identifying those people who can work above their pay grade as the Americans say. Some effort devoted to increasing the robustness of the telephone system or on developing a simple system for contacting staff outside working hours will go a long way to overcoming the human anxiety that can take place in the first 24 hours. Being able to access to your IT systems from other sites or even remotely will pay dividends enabling staff to work from home or almost anywhere. Having robust banking and financial arrangements to ensure that you can continue to pay employees and suppliers along with back up accommodation having already been identified is smart. None the least some drills carried out in conjunction with Emergency Services or local authorities are always informative. We have heard these simple basic strategies time and time again over the last two days.

What ever you tackle first, whatever continuity strategies you put in place, they need to be realistic. Physically moving staff and operations always takes more time than expected and has more impact on the available working day than expected. It is a little like that ancient rule for estimating time and space for any maritime activity at sea. Estimate the amount of time you need, double it and add some more and you will be close. Even with the clinical Recovery Time Objective it is important to allow sufficient restart time into the equation. If you are after true resilience then you clearly need either dual site operations or continuous availability solutions. In the event of an interruption at one site the business function is transferred to one or more alternate locations at which staff and facilities are already prepared to handle it. These options are amongst the more expensive to implement but they provide quick recovery. To be a viable recovery strategy this configuration should have geographical separation.

How far should an alternate recovery site be geographically separated from the primary site? Technology duplication at separated locations is obviously required when resumption timescales are tight, but the cost is substantially increased. The decision as to whether to duplicate or contract hardware and equipment in advance or simply to acquire these items post any incident must take into account the expected lead-time for acquiring the items. In a widespread natural disaster other less-prepared organizations may be chasing the same equipment. For this reason verbal promises by a supplier to keep a contingency stock should be treated as non-contractual. Current surveys which as to how far an alternate site should be from the primary site indicates the average

distance for hurricanes is 300 kilometres the highest average of any category, while conducting operations near a civilian airport has the lowest result at about 70 kilometres. Who thinks that doing business within 70 kilometres of Dubai airport is an acceptable risk? You may think different if you if you were at Dubai airport earlier in the year when the nose wheel collapsed on a Bangladesh Airlines plan causing massive passenger disruption for two days. Who here has an alternate or recovery site outside the power grid of the primary location? Who here has an alternate or recovery site in another country or more than 300km?

It is very important to check with service providers on connection times for telephones. The redirection of telephones to alternative locations may not be possible within an acceptable time particularly during a wide-area outage. Most telecommunications companies offer a range of flexible planned solutions that will allow instantaneous or rapid redirection of calls from one site to one or more alternatives. The logistical problem of handling telephone calls during an interruption once they have been redirected also needs to be addressed. Indeed outages are often typified by substantially increased volumes of calls. You can operate a mobile switchboard with hand phones although these frequently jam at the height of any Central Business District emergency. Even SMS towers clog up. The convergence of telephones and data networks such as Voice Over Internet Protocol is also creating new communications continuity opportunities. There are very sophisticated Internet based systems now on the market such as [www.missionmode.com](http://www.missionmode.com)

The monetary and non-monetary impacts that terrorism and natural disasters can have on an organization are clearly immense. After aircraft disasters it is a fact that up to 30% of employees do not come to work such are the stresses and strains and 5-10% of employees never come back. Recovery strategies based upon insurance can provide compensation for loss of assets, increased costs of working and protection for any legal liabilities. However it may not provide cover for the full expense of an incident or for damage such as the loss of customers, impacts on shareholder value or loss of reputation. You should work closely with whoever leads on tangible insurance matters. You can go for an all risks type policy which will compensate for the assessed value of the damaged or lost physical assets. Business Interruption insurance may also pay for either the increased cost of working during resumption or for loss of profits over the disrupted period. Key man insurance may provide a sum following the loss of named individuals while liability insurance may provide protection for financial liabilities associated with employees and third-party property and people.

Our experience is that an effective Business Continuity plan in the aftermath of an event of disastrous proportions is one that is simple, focusing on the basics with no unnecessary detail. A BCP is like a Swiss Army knife with lots of cool tools in a compact package. In case of emergency, grab this. We frequently find that early versions of plans contain much verbage as people get their head around what the subject is all about. Make them easy to read under stressful conditions with plenty of white space like a CV. Most people will only look at them once every 12 months at best. Checklists like a pilot uses are best. Sometimes the communications and notification parts of plans to customers, clients, contractors, visitors and the like are separate documents as this is managed on a corporate front and in other cases it is devolved to a line of business.

By now your heads are probably spinning and you are wondering how such readiness can be achieved? How do you pull it all together? Readiness can ultimately only be

achieved through adequate resourcing supported by budget cycles. Mature Business Continuity budgets equate to 1-3% of operating costs plus 3rd party contracts. Who here has BC budget of 1-3% of their operating costs? Most of you are probably thinking to yourself how great it would be to have control of a BC budget which represents of 1-3% of operating costs? For the vast majority of organizations how do you do more, instantly, under extreme circumstances of terrorism and natural disasters with leaner organizations? In an ideal world, with unlimited resources BC Managers would develop fully tested and comprehensive BCP whilst at the same time put together carefully chosen regularly exercised CMT. However, the reality is that for the vast majority of organizations, BCM activities are compromised by limited budgets and insufficient time and resources. Therefore prioritization must take. Is it better to try and focus on both the plan and the team or should one area be given the lion share of resources to the detriment of the other? Our advice is that the benefits fall on of the side of having a strong CMT although some BCP development is essential to ensure that the team has the necessary information and that the required pre-planned DR arrangements. This is the minimized plan and maximized team approach. Keep the BCP to the absolutely bare minimum with no complicated procedures and processes. Just simple information that the CMT can use at the basis of taking actions and decisions. Build the best team possible with your internal and external resources. Train the team and exercise it again and again. Ensure that each team member is backed up by a deputy and empowered to make all necessary decisions. Ladies and Gentlemen this is the most important slide that I will show all this afternoon. This is how you overcome the reluctance by senior management and other stakeholders in accepting the risk factors associated with such situations. If No Risk No Champagne is your business philosophy like some of the best companies in the work then your Management Team must be drilled in Crisis Leadership. Some say Crisis Leadership will become the dominant form of management in the years ahead.

If your business operates from more than one location how does this affect your BCP in response to terrorism and natural disasters? Virtual Crisis Management Environments are a very useful tool for storing and applying BCP and collaborating between different time zones and locations. When faced with a crisis, a crucial part of any BCP is locating, informing and getting feedback from key audiences, including management, response teams and employees. Many plans involve manual call trees or unsophisticated auto dialers to reach the people responsible for appropriate response decisions. Continuity Planners have found these approaches to be grossly inadequate in a major emergency and hence many VCME alternatives are now on the market and they are continuing to develop. All VCME seek answers to questions like how will we reach hundreds or thousands of people quickly during an emergency? How do we find and assemble response teams, particularly during off hours and weekends? How do we collect and analyze feedback for faster decision-making by key personnel during a crisis? Continuity Planners are also continuing to look for solutions that enhance communications throughout the initial response and subsequent recovery process, and not simply the initial notification phase.

There are many unique challenges to communicating after terrorism incidents and natural disasters, such as the plethora of devices by which people can be contacted, continually changing work schedules, situations that required certain people to receive one message while others received another and so on. Consequently VCME automate the complex manual call trees. And so it is that the Internet is now central in continuity planning, as it has for many other functional areas of organizations. This change enables

new levels of capability, supplying collaborative environment to a wide group of planners. With VCME any user can view the current state of any plan, at any location, from anywhere in the world, at any time of day or night. Desktop exercises easily involve remote staff and when an event happens, everyone has access to a current version of their plan elements via wireless web or desktop computer. Critical tasks are automatically pushed to team members for immediate action and response. Post-incident support is automated by pushing pre-established tasks and allowing an auditable trail.

VCME seek to optimize IT and Communications Systems through various combinations of Virtual Private Networks and portals to inform traveling managers and fixed email addressees for teams to allow 24/7 communications; different-time and different places collaborative systems for geographically separated teams such as [www.mssionmde.com](http://www.mssionmde.com) You can have toll free numbers set-up for public hotlines, switchboards, which allow for a cascading system of answering multiple calls by internal Call Centres to overcome log-jams in telephone communications. You can have dark websites which can be quickly activated to replace normal sites for media releases and fast facts. Despite all of this technology, and with such systems approach and virtual networking allowing organizations to fight above their weight, VCME can be manpower intensive, and organizations must always be prepared to go back to basics in crisis situations. For example, the crisis benchmark for posting media releases is one hour; a near impossible task without pre-programmed email and facsimile addressees but you must be able to do it from the car park. Computers in the Management Team Room can simply become Senior Officer Fascination Devices so VCME are no substitute for the mental wetware required to develop strategy and implement crisis leadership under pressure. Crisis leaders need to guard against these fascination devices, which optimize software and hardware, but which do not generate the bold and creative thinking required to control and transform from crisis situations.

Let me speak about terrorism for a short time. For 26 years I perfected the art of asymmetric warfare and for the last seven years I have been advising the Crisis Teams of global companies. Compare me to Osama bin Ladin if you like. We are the same age. We have similar backgrounds as engineers and as exponents of deadly violence. We have both destroyed many things and we have both worked in industry. That said, do not fall into the Business Continuity trap of thinking of him as a terrorist. If you consider him to be a business rival then you will have a chance of out maneuvering him in the Business Continuity sense. Al-Qaeda is run like a firm. Bin Ladin is a hands-on Chief Executive with a huge appetite for risk and a meticulous approach to his business strategy. Just think of Al-Qaeda a franchise in an economic fight to the death. Managing the Business Continuity response to a terrorism incident involves going head to head with the OBL Franchise. Emergency Managers must continue to look at patching the hole in the fence, and their plans and actions must be focused on getting back to the past – solid status quo. Crisis leaders however must see the open paddocks beyond the fence, and their strategy will focus on getting back to the future and the opportunities that await them. This is vision and it happens in the boardroom. This is extreme competition and exploiting the proactive stance, just as the preamble to the Al-Qaeda training manual says.

In the absence of direct access to government or actionable intelligence; if we are to have any chance of gaining the initiative in business, the focus must be on understanding the terrorist threat and getting inside the opponent's decision cycle. How

do you do that when you can only read articles in newspapers? Many businesses rightfully complain that the government has passed little back to them in return for their release of commercial vulnerabilities. The reality is that the information is there and it is available from open sources. CNN knows more than just about any police force. With this information you must learn to think like terrorists. You must develop your business intelligence collection skills and go on the offensive to make money. Beyond bin Ladin thinking is the only sustainable advantage in multi-competitor times. It is the only way of achieving a security dividend and generating return on investment. Business continuity is not enough to achieve reliance and within a few years, dare I say it, it may fade like all management fads as being unsustainable. A major Australian insurance company spends 5.5 million dollars on disaster recovery, but how much on defining the threat? The reality is that business cannot afford to harden everything and Business Continuity Plans cannot rely on mutual aid, so companies must conduct threat penetration testing themselves.

A simple example of threat penetration is when an Australian journalist walked into the Olympic Stadium in Athens before the Games and wandered around unchallenged before writing an article about the hopeless state of construction security. Terrorists do threat penetration testing on mobile phones all of the time as disruptions to air traffic across the Atlantic have shown. Maybe one of them is attending this conference. Camera men even managed to penetrate a headquarters in the early part of the war in Afghanistan and assassinated a guerrilla leader. Investigators frequently use deception to gain access and to elicit information within the confines of ethical conduct. Business must recognize, like terrorists do, that such intelligence equals edge. After all, what is the point of acting conventionally in business, when market secrecy is essential.

It is important to understand that Business Intelligence is more than Risk Management. The top companies will fight for both blue and red information. Blue business information is looking at yourself from a Blue perspective as well as looking at red. Blue information includes worst-case thinking, some of which may never actually occur. Red business information is looking at Blue from a red perspective. Red Cell thinking is looking at your company through the adversary's eyes. Frequency and severity form the language of risk, but threat is measured in terms of intent and capability, sometimes expressed as means, method and opportunity. It is one thing to have the marvelous ability to predict rain, it is quite another thing for Noah to build the Ark in time and save mankind. The application of Red and Blue Cell thinking will give you edge; enabling you to strike a balance and walk the thin line between safety and free movement of passengers and freight.

If you wish to interdict a terrorist operation before the attack occurs, you must train all of your employees to be vigilant and to collect intelligence. In short you must humanize security. It is not enough to use deception and to hide vehicles carrying dangerous cargo as cleanskins, or to have contractual Business Continuity clauses for third party interdependencies. You must humanize security through deliberate business intelligence collection to contribute to profit. Intelligence is better than technology any day. The only time that a terrorist attack can be prevented is in the planning stages. While most companies will never face a terrorist attack, preparations will also improve security against criminals and disgruntled employees. The Al-Qaeda manual claims that it is possible to gather at least 80 percent of information about the enemy, that is business, from the Internet. You are then well advised to scrub publications and Web sites of critical information. In conducting an appreciation of your business from an OBL

franchise perspective, you will not interdict the hiring phases of a terrorist operation, but you may well detect their elicitation of information. Al-Qaeda operatives are meticulous, even obsessive in surveillance. They understand that infrastructure is vulnerable to cyber and physical disruptions. For example it is a tactic for their operatives to make anonymous threats via telephone and email then to monitor the response. They are trained to act as people who work on the streets; they watch and they learn. Targets are not chosen randomly. Like organized crime they obtain information through infiltration and well-placed informants. They work in isolated groups and communicate covertly.

It can be difficult to assess intent and capability when the terrorist functions from cells, but you can look at your own assets, and this is what they do. They will use something like the CARVER acronym; and when looked at through red eyes the threat can become a little clearer and help determine whether you are a soft target. This is how you evaluate risk events that may occur during terrorism. It also has some applicability to low probability and high impact events like natural disasters. C is criticality or relative importance. What part of your business is most critical? An adversary may seek to destroy a Disaster Recovery Centre, a Hot Site, in a capital city or critical blood stocks, in addition to key communications nodes. A is for ease of access. Just getting to the target can be confusing at best in the middle of the night in unfamiliar terrain and urban geography; so easy access targets are often preferred. The terrorist may simply turn up in a taxi. Suicide terrorists aside, they do not want to be caught in the act. They will take the path of least resistance and go to places that do not have people who are looking for things that are unusual or do not have adequate visible patrols. R is recoverability. How easily the asset can be brought back on line. This downtime thinking may indicate a further threat to repair and spare parts facilities, as a rival will seek maximum outage or maximum bang for buck. V is for vulnerability and the ease with which people and infrastructure can be put out of action with a hammer or a computer virus. Fire, flood, and kinetic energy are all considered. Martyrs are just as scared as anyone else when it comes to delivering the final blow, even with the motivation of 70 virgins and a place in heaven. All terrorists will look for the easier way. E is for effect. Terrorists will concentrate on targets that will cause the greatest adverse effect on population; to get the entire nation to go into mourning. Mass fatality attacks are a hallmark of al-Qaeda tactics. They look for maximum impact and devastation and attacks in waves as has been demonstrated many times. R is for recognition. The what is it, and the what-where type questions? The ability to actually to identify one target from another.

Just how vulnerable are you to the OBL franchise? Test yourself. Attack yourself. Gates and guards, guns and dogs are not impediments to intelligence collectors. If you want to protect yourself you are going to have to rely on far more than that. In addition to threat penetration testing, the gathering and assessment of Intelligence can provide indicators or warnings about exposures and opportunities. A good example of how this can work come from when we were preparing plans for a company in Indonesia. We established a small team to assess the political, economic or social triggers that might call for a drawdown plan to be initiated. By putting very simple collection and reporting procedures in place, the company found significant business opportunities.

Ladies and Gentlemen, if you want to achieve market superiority over a competitor such as a terrorist, you must refocus on cost leadership and differentiation of product. Cost leadership only comes from achieving the security dividend, by humanizing security. Differentiation of product only comes from insisting on equal business resilience from your suppliers and providers.

Ladies and gentlemen in recovering from terrorism and natural events where to from here? As explorers of business continuity, to practice problem-solvers you must be given problems that you have not solved before. Many of you will have seen the Master & Commander movie starring the Australian actor Russell Crowe. For those that have not, picture a British war ship, a sail ship from centuries past out there in the fog looking for the French. The Captain is below and the Junior Officers are up on the quarter deck. One of the junior officers thinks he hears something (cup my ear). He is uncertain but he fears a French Frigate. He cannot see the enemy but he decides he must act. Someone must go and tell the Captain. Next minutes the alert, call out the guard. And so it is with business continuity. All of us are that guard in that fog. We work best in a disaster. Like the best racing car drivers, we practice in the rain. We want to be good in the rain because we want to win. Even the good Admirals must practice, because even the best Admirals only win 3 out of every 5 battles.

Just as the world has come to terms with terrorism and natural disasters so have the best companies learnt to use their crisis leadership capability to be able to Eskimo roll their canoe in whatever sea they choose to paddle, and to take their companies beyond danger to opportunity. The future is for sale and it is all about surfing on the front of the wave instead of being in front of the iceberg. The better companies have moved from Emergency Response to Crisis Anticipation. The best companies are re-designing themselves around Crisis Leadership. Leadership is the best thing that you can do before and after terrorist incidents and natural disasters. This approach is looking for the next jungle, not just sharpening the machete or checking the compass in the current one. Crisis Management is just looking at the hole in the fence. Crisis Leadership is seeing the open paddock beyond. It is one thing to have a plan, it is another to practice it. Like the Al-Qaeda manual says, do you have any questions about how these battles are fought and must be won?