WHAT DO YOU DO WHEN TOO MUCH BUSINESS CONTINUITY IS NOT NEARLY ENOUGH?

Strategies to deal with the threats posed by terrorism and natural disasters

The word is rapidly becoming a scarier place. Investors reaction can certainly amplify the impact on the recovery. Torsten Slok Chief international Economist Deutsche Bank Securities New York in response to the disaster in Japan. It has been almost sixty years since businesses in Sydney and Newcastle were directly under attack by submarines. With climate change continuing to manifest itself in floods and violent storms and the Internet allowing terrorists and citizen journalists significant advantage, what you do when even with the best resilience that money can buy it just does not seem enough? Some say that Wikileaks is an information weapon designed to control global superpowers. Do you bother doing anything at all about the impacts of security events or natural disasters?

The fact of the matter is that mass casualty plans are now a standard response as terrorism puts every public gathering place at risk. Responding appropriately in the first 15 minutes with scoop and run tactics is when First Responders have most impact in saving life. All companies have Employee Assistance Program service providers on call and the best companies have well developed systems for providing peer support. It is now normal to store emergency contacts for all employees in melt proof safes and to have duplicate copies off site. The best companies continually account for all people and are able to do immediate name calls and head counts if evacuating facilities. Invacuation by staying on site with the air conditioning off is as important as traditional evacuations when dirty bombs or toxic gas are involved, although any informed decision to stay or go can be near impossible to make. In high-rise buildings elevators maybe the fastest way out regardless of warnings and if it is earthquake the farther you are inside the building, the greater the probability that escape will be blocked. But how will you know if is a dirty bomb or an earthquake? Virtual crisis 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 disruption through the use of internal Call Centres and hotlines to contact employees. Finally common points of contact in the event of an emergency, sometimes referred to as rally points, are essential for business as is a community system for lost communications, lost communications procedures for travelers and GPS tracking of assets. …….. Wow! … Who here can do all that?

What do you do when the response is over and you find yourself starting from Ground Zero after the dark shadow has passed? It highlights the criticality of factoring in viable re-start times to plans, before Recovery Time Objectives kick in. From an insurance perspective it is important to match deductibles to realistic re-start times and to consider cover for extreme risks. It is also fundamental to have a crisis team in place. It is still surprising the number of companies that do not have a simple plan for their leadership to meet in a primary or secondary location or virtually. 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. Having robust arrangements to ensure that you can continue to pay employees and suppliers along with back up accommodation is smart. None the least some drills carried out in conjunction with Emergency Services are always informative. Whatever 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 it has more impact on the available working day than expected. Who here has rehearsed the viability of re-start times after black swan scenarios?

An effective plan in the aftermath of an event of disastrous proportions is one that is simple with no unnecessary detail. Early versions of plans frequently contain much education 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. If you are after true resilience then you clearly need either dual sites or continuous availability. To be a viable strategy there should be geographical separation. Current surveys as to how far an alternate site should be from the primary site indicates 300km for cyclones while conducting operations near an airport is about 70 kilometers. The redirection of telephones to alternative locations may not be possible within an acceptable time particularly during a wide-area outage and the logistical problem of handling telephone calls during an interruption once they have been redirected also needs to be addressed. Walk your optic fibre if you have VPN. Who here has done that? 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 emergency. Even SMS towers clog up and there is a need to map them. .. Who here knows where they are? The convergence of telephones and data networks with VOIP creates new continuity opportunities and there are some very sophisticated Internet systems now on the market.

Mature continuity budgets equate to about 1-3% of operating costs but for the vast majority of organizations how do you do more, instantly, under extreme circumstances with leaner organizations? In an ideal world with unlimited resources there would be fully tested plans with carefully chosen, regularly exercised teams. The reality is that for the vast majority of organizations planning is compromised by limited budgets and insufficient time. Is it better to try and focus on both the plan and the team or should one area get the lion's share? Our advice is that it is best to have a strong team although some planning is essential. Keep plans to the minimum with no complicated procedures; just simple information that teams can use at the basis of taking action. Build the best teams possible with your 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. If *No Risk No Champagne* is your strategy like some of the best companies in the world then your team must be drilled in Crisis Leadership. Some say Crisis Leadership will become the dominant form of management in the years ahead of just in time business, incredible supply chain dependencies and tipping point scenarios when two or more sectors are in melt down.

Virtual Crisis Management Environments are a very useful tool for storing plans and collaborating between different time zones and locations. 40% of the world's information goes through India year day and the world awaits I2K, an IT event of Pearl Harbor

proportions. A crucial part of invoking any plan is locating, informing and getting feedback from management, response teams and employees. Many plans involve manual call trees to reach people; often grossly inadequate in a major emergency. Hence many VCME are now on the market and are continuing to develop in order to be able to reach hundreds or thousands of people quickly during an emergency and collaborate. .Who here uses a VCME like this?

There are many challenges to communicating after terrorism and natural disasters such as the plethora of devices by which people can be contacted, continually changing work schedules and situations that required certain people to receive one message while others received another. VCME automate these complex manual call trees. And so it is that the Internet is now central in continuity planning, supplying a collaborative environment to a wide group. 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. You must have two Internet service providers. When an event happens, everyone has access to current plans via wireless web. Critical tasks are automatically pushed to team members for immediate action. Post-incident support is automated by pushing pre-established tasks and allowing an auditable trail. Such VCME seek to optimize IT and communications systems through various combinations of virtual private networks and portals to inform traveling managers and fixed email addresses for teams to allow 24/7 communications; different-time and different place collaboration for geographically separated teams….. In the land of the blind, the one eye man is king.

Despite all of this technology and virtual networking allowing organizations to fight above their weight, VCME can be e-power intensive, and organizations must always be prepared to go back to basics; even runners and hand held radios. For example, the 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 generate such information from the car park. Computers in the crisis room can simply become Senior Officer Fascination Devices so VCME are no substitute for the mental wetware and physical sweatware required to develop and implement strategy in teams 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. It is said that businesses become truly resilient, the ability to withstand, recover and build from debilitating business shock when they put people first, when they use diverse internal resources and when they effectively coordinate with all external parties. Who thinks that is true?

Implementing strategy in response to terrorism involves going head to head with OBL franchises. If you consider terrorism to be a business rival then you will have a chance of out maneuvering them in the business continuity sense. Al-Qaeda is run like a firm with a huge appetite for risk and a meticulous approach to business strategy. Just think of terrorism as a franchise in an economic fight to the death. In this environment Emergency Managers must continue to look at patching the hole in the fence and their actions must be focused on getting back to the past, 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 Al-Qaeda training manual says.

In the absence of actionable intelligence if business is to have any chance of gaining the initiative the focus must be on understanding the threat and getting inside their decision cycle. How do you do that when you can only read articles in newspapers? 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. Beyond bin Ladin thinking is the only way of achieving a continuity dividend. Business continuity is not enough to achieve resilience. The reality is that business cannot afford to harden everything and plans cannot rely on third parties, so companies must conduct threat penetration testing themselves. Terrorists do threat penetration testing on mobile phones all of the time as disruptions to air traffic have shown. Business must recognize, like terrorists do, that such information equals edge. Who here does threat penetration testing?

If you wish to interdict terrorism before the attack occurs you must train all of your employees to be vigilant and to collect intelligence. It is not enough to use hide trucks carrying dangerous cargo as clean skins or to have contractual Business Continuity clauses for third party interdependencies. 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 other threats. The al-Qaeda manual claims that it is possible to gather at least 80 percent of their information from the Internet. You are well advised to scrub publications and websites of critical information. Who here has a business intelligence collection system? Who here looks at their website from a threat perspective?

Just how vulnerable are you? Test yourself. Attack yourself. In addition to threat penetration testing, the gathering and assessment of Intelligence can provide warnings about exposures and opportunities. If you want to achieve market superiority, you must refocus on cost leadership and differentiation of product. Cost leadership only comes from achieving the continuity dividend, by humanizing security. Differentiation of product only comes from insisting on equal business resilience from your suppliers and providers. Who here has ever conducted a penetration test of their company? Perhaps even just a secret shopper?

Like good strategy, Crisis Management begins before the first move. In coming to terms with terrorism and natural disasters the best companies use their Crisis Leadership capability to take their companies beyond danger to opportunity. 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. You must learn to out run the bear or at least to run faster than the person beside you. Like the Al-Qaeda manual says investors can rightly ask how will companies fight these battles and win?