

BEYOND BIN LADEN THINKING – THE SECURITY DIVIDEND

24 August 2004

In the next 48 hours, the ride will get rougher. 4800 Australians will be involved in a road crash, 550 will be injured and five will die. Hard hitting statistics by any measure and ones that are non discriminatory. It can be a person you have never heard of, the person next door, your family, your colleagues or you. This outcome could equally be the result of a dirty bomb here at Darling Harbour. Just as we have adjusted to the road toll, so has the business environment changed forever with the best companies learning to use their corporate 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.

For 26 years I perfected the art of unconventional warfare and for the last four years I have been advising the Crisis Teams of Australia's publicly listed 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. I have had him in my sights in Kuwait in Indonesia and in Homebush bay, as he has probably had me. That said, do not fall into the 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 manoeuvring him. 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 with the capitalist west.

Managing a security crisis involves going head to head with the OBL Franchise Crisis Team. 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.

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 casualties and improving communications. Mass casualty plans are now standard as terrorism puts every public gathering place at risk. Responding appropriately in the first 15 minutes is when you will have most impact in saving life.

All companies have Employee Assistance Providers on call, and the best have well developed systems for providing peer support or fast buddies to use the expression adopted by Singapore airlines. 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. The best companies continually account for all people on site and are able to do immediate name calls and head counts if evacuating facilities.

Invacuations, staying on site with the air conditioning switch off, is equally important as traditional evacuations when dirty bombs are involved. In high-rise buildings elevators may be 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. Loudhailers are as important as ever in addition 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 travellers, GPS tracking and security clearances to open channels of communication. Do you think we need a national emergency readiness standard for business, as an extension of national liquid fuel ER plan? Should it be voluntary, or a factor in obtaining terrorism insurance?

Islamic governments have never and will never be established through peaceful solutions and cooperative councils. They are established, as they have always been by pen and gun, by word and bullet, by tongue and teeth. It is through both means that the battles are fought and must be won. Up until now, the conference has focussed on consequence and the reactive response. I will pick up where Clive Williams left off as 90% of any effective appreciation is about the 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 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 information. The reality is that the information is there and it is available from open sources. CNN knows more than any SE Asian 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 it will probably fade like all management fads as being unsustainable. IAG 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 industry 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 some months ago 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 recent disruptions to air traffic across the Atlantic have shown. Camera men even managed to penetrate a guerrilla headquarters in the early part of the war on terror in Afghanistan and assassinate him. 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 to build the ark in time. 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.

Phases of a Terrorist Operation Cell and Networks, Recruiting, Selection, Training and Indoctrination, Establishment of Cover and Authentication, Positioning by close-access connections and establishment of Cover on the Spot, Surreptitious Acquisition of Information, Communications and meetings with informants and Couriers, Passive and active killing. 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 interdependencies. You must humanise 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 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.

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.

The knowledge necessary to defeat your opponent exists in your organization, and you just need processes in place to extract and share vital information with everybody who can benefit. The single most significant step you can take to increase the value of information is to increase the speed with which it is acquired and acted upon. Most companies are not organized to collect and act upon information in a disciplined way; and the most important employees, the ones with the contextual understanding of the situation, must be empowered to act on information.

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.

If you want to achieve market superiority over a competitor, even 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 business resilience from your suppliers and providers. The Sears model shows that if you pass information in this way that there is a direct correlation with profit. If you want security to become a contributor to profit, a profit centre and not a cost centre, you must implement formal intelligence collection now, empower all employees to collect, and start analysing. Fraud and misappropriation of assets affects 50% of Australian companies and you will be surprised what you find. Small companies can collect it and use it just as well as large companies. Once you have got it, protect it like you protect anything else that helps you increase profit.

In the business game tomorrow we will practice participants in blue and red techniques so that they can work out what the OBL franchise is going to do and we will test our response in a simulation. Like the Al-Qaeda manual says, do you have any questions about how these battles are fought and must be won?