

RIDING THE TIGER – FOREWARNED IS FOREARMED

The reality is that the game of business is played in a jungle and not on a playground. Thus the rules of the jungle prevail

Al-Qaeda is essentially an adversarial franchise in an avowed economic war to the death with the Christian capitalist west. Bin Laden says that he will send the US broke, so what will be next? Small planes flying into bigger planes; ships driven into facilities on and offshore

Petrol tankers driven into terminals; toxic and combustible gas clouds released in confined spaces; foot and mouth disease or smallpox pandemic; indiscriminate shooting and suicide attacks in lieu of escape; LPG gas bottle bombs; and a virus on a control system are some of the most underemployed methods around, and indicative of what the OBL franchise maybe planning. Some are obvious and some may require you to think outside the box, more like a screenwriter or novelist. In this interactive session, you collectively represent the Management Team of the Sydney Convention & Exhibition Centre and you have an extract from your website on the table. For the next 15 minutes we will think like a deadly competitor, be the OBL franchise or a business rival and attack ourselves.

In order to leverage our knowledge from a red perspective, and ability to attack deadly competitors I want you to sit on the other of your table and face the back of the room. Red thinking is looking at your own organization through the competitor's eyes. We are now on the outside and looking back in. We need to devise a terrorist plan to attack the Sydney Convention & Exhibition Centre. Please complete the red worksheet as we go.

It is important to understand the meaning of counter-intelligence, red thinking, and not to confuse it with security, blue thinking. The formal definition of counter-intelligence is active measures, sometimes taken in conjunction with federal agencies to identify and neutralize the intelligence-collection activities of a business rival. It is all about working out what the opposing intelligence officer is going to do. It is seeing through the eyes of the adversary, by emulating their approach through legal and ethical threat penetration testing.

What and why does the competitor want to know about our vulnerabilities and strengths?

How would they go about finding out and collecting such information? Once such information is known, what are their most likely options for what strategy? Of such options, what may be their most likely course of action? This is what a counter-intelligence officer thinks. You think like OBL. Because terrorists like any competitor are adapting to new security measures and counter measures, it is always important to conduct an appreciation from a competitor's perspective; to work out what the other guy is thinking. This process starts with an analysis of your organization, your people and your facilities. For example, like the Westfield shopping centre at Centre Point Tower, are you a social, cultural or economic icon whose destruction would serve terrorist goals? This questioning allows you to determine what to protect, how to protect it and how long to protect it for, as no organization can stay in business if it keeps its products and services under lock and key.

C is criticality or relative importance;

A is for accessibility or ease of access;

R is recoverability and how easily the asset can be brought back on line;

V is for vulnerability and the ease with which people can be impacted;

E is for the effect on the local population;

R is for recognition and the ability actually to identify the target.

In thinking red you can use this simple CARVER assessment to identify your vulnerabilities so you can determine where you will most likely be attacked.

Implementing Countermeasures - Employee awareness through elicitation training, document management and background checks. Physical/electronic safeguards (security) and penetration testing. Finally at the end of the red process, these are the sort of countermeasures that you may consider implementing. Employee awareness is explaining to them how they may be exploited for information so that they are in a much better position to recognize approaches that maybe suspicious or at least reportable. This leads to employee participation and the handling of employee reports of suspicious contacts whether by telephone, email, while travelling or at trade shows or professional meetings. In terms of background checks, some studies claim that 75% of educational claims are exaggerated or created. Controlling documents from registration through to shredding is an important aspect as is locking of rubbish bins, plain clothes, sweeping of meeting rooms, use of encryption software and conscious use of mobile phones.

Now we want to think blue for 15 minutes. Please go back to the normal side of the table and face the front. We want to design a Security Management System including an Intelligence collection plan for the Sydney Convention & Exhibition Centre.

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. The only time that a terrorist attack can be prevented is in the planning stages. There is a limit to what can be done against the most extreme forms of attack and I re-emphasize that the only time that a terrorist attack can be prevented is in the planning stages. While most companies and organizations 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.

So that there is no confusion, this is how blue thinks. Blue business information is looking at your self from a Blue perspective as well as looking at Red. Blue information includes worst-case thinking, some of which may never actually occur.

This is what Corporate Security Officers are doing. They continually assess threat in terms of intent and capability. Intent is desire; expectation. The degree to which they demonstrate competition or intelligence collection against you. It is measured in terms of their history and current activities and success is largely dependent on your perception of the threat's ability to overcome your security controls. Capability is resources and knowledge; their modus operandi, finances, and opportunities available to them; their organizational presence and location. Their technical and professional skills.

The gathering and methodical assessment of business intelligence is a critical tool as this assessment can provide indicators or warnings of exposures and entrepreneurial opportunities. The majority of this information resides in the public domain, and harvesting its value is simply a matter of accessing it in a systematic way. Business intelligence collection is less a matter of penetrating secrets and more a matter of separating useful information from open legal and ethical source information. Future value must be linked to business taking risks through business intelligence gathering. The single most significant step an organisation can take to increase the value of the information it collects is to increase the speed with which this information is acquired and acted upon. Most employees are not trained, equipped, or organised to collect, process and act upon information; conversely, those employees with a contextual understanding of the business situation, are not always empowered to act on information, and would not normally receive intelligence products. So how do you as a manager collect, process and disseminate this information? This is the format that drives collection.

You simply state what it is you need to find out. A yes/no request is great if it can be stated that way or it maybe commercial information that you are after. Indicators and warnings cue the collector in locating the information be it advance knowledge of a competitive product being launched or the signal of a hostile takeover or emerging industrial relations issue. The sources are those who you know are more than likely have the information you want. Allocate about thirty per cent of effort to human sources, twenty per cent to hard copy and fifty per cent to online services, including imagery, radio and television broadcasts. Specify how you want the information for example as a statistic, or some other quantitative value or an actual sample of the product

Finally specify the time by which you want the answers in order to evaluate the information. It is that simple.

Finally this is the structure of a Security management System, which even for a large organization may only be less than about ten pages of text. If you want to turn security from a cost centre into a profit centre, a tool for driving the organization more efficiently then this is what must be done. For example tracking containers in transit for security reasons ca also be used to map the logistic chain and save money. Planning the identification of threats, their assessment and control requires you to identify any legal and statutory requirements, to make a statement of realistic objectives and how it will integrate into other management systems. Implementing is about putting structures in place and allocating resources, responsibility and accountability, lines of communication and reporting. Training maybe required to particular competencies. Threat evaluation and control is the crux using tools we have already described and stating what normal controls consist of, and actions on losing contact with a facility or person, a terrorist Incident actually occurring or increased levels of threat along with the appropriate Emergency Response. Monitoring and Measurement requires a description of procedures for investigations, record keeping and auditing.

In defeating commercial rivals and security threats alike, countering their intelligence gathering is much more than Risk Management. Top organizations fight for both blue and red information as part of a structured Security management System. The application of Red and Blue Cell thinking gives you edge. It is one thing to have the marvelous ability to predict rain, it is quite another thing to build the ark in time. It has been a fast and furious minutes 30 at the end of a long two days. Do you have any questions of me?

----- END -----