mi2g

Asymmetric Warfare

Business Continuity in the Face of Terrorism

Lloyd's of London, 14th November 2001

Keynote Speech

DK Matai - Chairman & CEO – mi2g

Introduced by Dr Simon Moores, Chairman, The Research Group

Ladies and Gentlemen

Although the recent air-crash in New York was most likely due to engine malfunction it reminded everybody of the horror of 11th September. As we watched the crash images a second time on 12th November - with some sense of trepidation - a few thoughts crystallised on the logic of terrorism:

1. Our way of life in the interlinked world is much more vulnerable than ever before
2. Terrorism is a sophisticated activity and has to be dealt with strategically
3. Post the collapse of the Soviet Union, terrorism could continue to fill the power vacuum
4. Modern life is susceptible to terrorism as a blunt expression of conflict and protest
5. There are specific and collective counter-measures, which we can put in place to mitigate the threat to our way of life.

Businesses need to be able to carry on functioning despite interruption. However, if they suffer loss of critical assets on the scale of 11th September, the most meticulous disaster recovery programmes and business continuity procedures can cease to deliver.

Business confidence has been hit post September 11th. In order to shore up the willingness to invest, the US Federal Reserve and the Bank of England have cut their interest rates to the lowest for 40 years. If Japan's experience is a guide we could face a decade of deflation. Both Sir John Templeton and Warren Buffet have suggested an eight-year downturn.

Insurance and Reinsurance

Risk managers and organisations' perception of risk have changed. The insurance and reinsurance companies that were involved in covering life, property and casualty, including business interruption and liability, have had a see-saw movement in their share price since 10th September. In the immediate aftermath of the tragedy, the market capitalisation of Swiss Re, Munich Re, AIG, Chubb, Allianz, Axa and other global insurers fell by double digit percentages. This was to be expected as the estimates for the disaster rose, reaching USD 40 Billion. Last week, Warren Buffet told shareholders of Berkshire Hathaway that the full extent of 11th September would not be known for years. This statement has two implications:

1. The loss from 11th September, including legal costs, may be much larger than we now estimate
2. Property insurance is no longer a short-tail line of business in these mega-loss scenarios

It is a popular nostrum that Casualty business is "long-tail" (meaning late or delayed development of loss) and Property is "short-tail" (meaning the loss is known right away). Losses like 11th September turn these traditional notions on their head. The business interruption and contingent type losses will not be known or worked out for years.

11th September has been like a light switch being flicked; it has happened that quickly. We are now in a HARD CYCLE – harder than 1985-1986; the descriptive "still hardening" for insurance pricing no longer applies. As a result, in the last few weeks most insurers have climbed way above their share price levels prior to 11th September. This is not a bad performance given that the sector is absorbing one of the worst losses and loss years in history. However, it is worth noting that insurance cover, for example, for airlines – in certain cases - has risen by between 400% and 1000%. The impact of these changes is six-fold:

1. There is an increased demand for insurance in areas where there is less appetite to accept risks
2. Premium rates are rising dramatically
3. Policy terms and conditions have tightened significantly post terrorism
4. There is severe limiting of capacity because of man-made and natural disasters
5. Scarce insurance capital is having to be allocated to interlinked risks
6. The many newly formed insurance entities in Bermuda like ARCH Capital, AXIS Specialty and DaVinci could take market share from Lloyd's and the London market

The financial stability of insurers is being further enhanced by Government policies to cover a large proportion of future terrorism both in the model of Pool Re in the UK, which was established in the mid-90s and the US House bill proposal to cover 90% of terrorist losses above US$ 20 Billion.

Mega-structure Risk

With the casualties, the horror and the shattering of US assumptions about themselves, **nothing** will be as it would have been. What we are facing by way of risk post 11th September is much more a mega-structure risk rather than an individualised risk. For example, if the electricity and telecom grids powering the City of London or New York fail, the business interruption is not just to one business. Several thousand organisations simultaneously face calamity. The entire command and control operations of a metropolitan environment depend on the critical matrix of energy, utilities, logistics and communications. This is the kind of interlinked mega-structure risk that requires further deliberation today, both from the public and private sector point of view, and *many of the illustrious guests gathered around the table tonight will have their views on this issue.*

We have to contemplate mega-risk not on the basis of a specific address or site but as a postal pin-code or perhaps several postal pin-codes simultaneously damaged. (Zip-code in America.)

Critical Infrastructure Intrusion

I would like to share an example of critical infrastructure breach. Last month, Vitek Boden of Australia was found guilty of hacking into the Queensland computerised waste management system and causing millions of litres of raw sewage to spill out into local parks and rivers. Boden had conducted a series of electronic attacks on the sewage control system after a job application he had made was rejected by the area's Council.

Financial System Risk

The financial system and hence our way of life is more vulnerable than we think. Increased hacking activity directed specifically at Western financial interests was reported by the FBI's National Infrastructure Protection Center (NIPC) in mid-October. A prominent hacking group said, *"the best way to earn money in a world under the control of financial markets is to attack the image, the reputation and the financial information that defines an enterprise."*

The banks are the last bastion of old, closed-source security systems. The IBM 4758 Crypto-Processor is used by many banks to encrypt sensitive data and the original source code remains undisclosed. The 4758 Crypto-Processor is military grade hardware and one needs a license just to possess it.

Your bank card PIN number – the 4 digit code that you have memorized for drawing cash out of the ATM - is encrypted in the 16 digit credit card number on the front of the card using encryption software running on your bank's crypto-processor. It took IBM 2 years and 100s of scientists spending 10s of millions of Dollars to develop the 4758 Crypto-Processor, which took

just two weeks to crack. In April 2001 at a conference in Paris, the vulnerabilities of the IBM 4758 were published. Dissatisfied with IBM's response to the exposure of the vulnerabilities, the Cambridge University Computer Security Group (CSG) have now published the code-breaking research on the web.

Using this information, it is possible for a dishonest, suborned or dissatisfied branch bank manager to use the Combine_Key_Parts permission to assist a crack of the Crypto-Processor over two days using just US$ 1,000 worth of hardware.

Computing Power versus sophisticated hacking

What this shows is that people are the strongest and the weakest security link. What one team of men can design another can reverse engineer. Given that high performance computing power is getting cheaper with each passing quarter, the capability of a hacker keeps rising.

Biological warfare and hoaxes

The multiple Anthrax cases, which are paralysing parts of the United States national physical communication infrastructure, are leading to a re-examination of the benefits of digitisation. Digital means are now perceived as safer than traditional snail-mail. This reinforces arguments in favour of electronic payment systems*, and the question I would like to ask all of you is what happens if the digital infrastructure that carries the electronic messages and payments now fails?*

Asymmetric threats

Any threat, which is disproportionate, such as the risk of a small group attacking a large country or a few individuals killing thousands is described as asymmetric. The perpetrators of terrorism on the US were a group of individuals with different nationalities and a common cause. About 20 of them ended up killing over 5,300. The ratio is 1:250. All the power of a nation state cannot deal with the speed and stealth of such a small sophisticated and motivated team mounting an asymmetric attack.

With the American Declaration of Independence in 1776 and the French revolution in 1789 arrived the modern concept of a nation state with all the rights for her citizens enshrined in the constitution. The sovereignty of the nation state is now being superseded by the sovereignty of the individual partly because of access to low cost travel, communications and computing power. Bin-Laden's supporters are from all over the Muslim world, from Indonesia to Algeria.

In the 21st century, asymmetric warfare is multi-dimensional. It is fought on land, on the seas, in air as well as through cyberspace.

The new dimension of asymmetric attack is cyberspace.

Cyberspace has made history out of geography and has unified people regardless of where they are.

Cyberwarfare's first pivot is as a community fragmenter / propaganda machine

In the battle for hearts and minds, the Al-Jazeera satellite channel is able to reach over 1 Billion Muslims. In the Gulf war in 1990, CNN was the main conduit of minute-by-minute information. The Arabs were getting information from CNN just like the rest of the world. It was easier to control public opinion then. This time round, Osama Bin Laden and his accomplices are using Al-Jazeera and so are other zealots mixed in with credible Arab and Western leaders. The US and UK may be winning the aerial bombardment war but the battle

for hearts and minds is controlled in part by Al-Jazeera. Their commentators speak from a faith point of view, which is more convincing and appealing to an Islamic audience in comparison to the BBC World Service and CNN.

Cyberwarfare's second pivot is attack and counter-attack on digital systems

The damage that an asymmetric electronic attack can do to our industrialised society is greater than what could be inflicted on a developing or under-developed country. Afghanistan need not fear an electronic attack but we have to be ready for it.

Recent attacks

According to the FBI's National Infrastructure Protection Center (NIPC), in the aftermath of the 11th September attacks, hacking groups have formed and participated in pro-US and anti-US cyber activities, fought mainly through web defacements. NIPC believes the potential for future Distributed Denial of Service attacks is high. The protesters have indicated they are targeting web sites of the US Department of Defense and organizations that support the critical national infrastructure of the United States, but many businesses and other organizations — some completely unrelated to the events — have been victims in the last two months.

The G-Force Pakistan defacements carried the message that in the coming month they would deface 1,500 US, British and Indian websites. The group also said that it had highly confidential US data that will be given to Al-Qaeda and the group also warned of an Al-Qaeda Alliance Online involving other hacker groups, which it said would start attacking sites.

Defence expertise

Historically, politicians in the US and UK have challenged their defence forces to provide adequate defence capability within limited resources. The focus has been on the physical dimensions – land, sea, air and outer space – and not on cyberspace. There is no defence capability for sustained counter-attack in cyberspace.

Cyber warfare poses threats directly to lower level infrastructure in all government departments and commercial institutions. It is unrealistic to expect the Ministry of Defence, or the Department of Defense in the USA, to provide 'defence' against such threats and, in any case, the expertise needed is relatively fast moving and cannot be 'trained' into people over a short period of time. The expertise lies with those who understand the technologies used to pose the threats, gained through experience, such as electronic attack and counter-attack specialist defence companies. All this may change in the years ahead post 11th September.

High profile attacks on economically sensitive targets

On 5th February 2001, the computers of the World Economic Forum were hacked by anti-globalisation activists. The culprits stole 80,000 pages of sensitive personal information such as cell phone numbers, eMail addresses, passwords and 1400 credit card numbers of forum participants, including UN Secretary General Kofi Annan, former US President Bill Clinton, Israel's Shimon Peres and Palestinian leader Yasser Arafat and Microsoft's Chairman Bill Gates. This electronic security breach contrasted sharply with the impenetrability of the Davos conference centre, which was protected by roadblocks and barbed wire barricades.

Low profile attacks on economically sensitive targets

The much more scary attack is a subtle manipulation. On October 3rd last year a Dutch hacker, Gerrie Mansur of Hit2000, warned NASDAQ and CBS's Marketwatch.com that he

could have altered their web sites in a subtle way. Mansur gained access to the global.asa file, which contains the global settings for the applications.

What happens if terrorists use a Mansur type vulnerability exploit to buy and sell options by subtle share price manipulations that are not declared public? Or change words in particular reportage on the digital media?

Two months ago, on 24th August NASDAQ halted trading in Brass Eagle's stock (XTRM) after a hacker broke into Brass Eagle's computer systems and mass eMailed hundreds of press releases containing fake financial statements over the Internet.

The single biggest failing of 11th September – fragmented intelligence

The single biggest failing of Western Intelligence Agencies in not having picked up the 11th September attacks is their fragmented electronic intelligence gathering systems, which have no capability to unify knowledge management and analysis. *Consider the number of different intelligence agencies in any one country involved in the collection of data - both overt and covert - in the modern democratic world. Consider the exponentially increasing volume of that data and the nature of it: voice, image, video, fax, text and symbols – both hidden as well as encrypted.*

It is an Herculean task to collect, sift, analyse and act on this intelligence data if the key pieces of knowledge are not to be missed. This cannot be done manually and we need smart technology solutions to help us. If the threat and targets are international, the Allied countries' knowledge management and analysis systems handling intelligence data need to be able to talk to each other. This has not been true for Agencies even within the same country, especially the US, who up until now jealously guard their own information. They do this to safeguard the reputation and budgets of their own organisations. This has to change; this is outdated thinking after 11th September.

One country cannot go it alone

So one of the greatest needs before 11th September was for upgraded secure knowledge management and analysis systems that were interoperable across Agencies within one country and between countries. That need is now paramount. The US, UK, most of NATO as well as Australia and New Zealand need to have interoperable Knowledge Management and Analysis Systems (KMAS) and tools for mining intelligence data. These new KMAS tools need to be able to cope with other countries of Eastern Europe, the Middle East and Asia.

Human intelligence

The next question to consider is how does one deploy people with the Knowledge Management and Analysis Tools to outsmart the malevolent people who are one step ahead and constantly figure out ways to outsmart the system?

The reality is that 70% of all complex attacks take place through insider knowledge and assistance and not political activists who go it alone. Disgruntled employees in sensitive places have been suborned, coerced, brought into believing in some faith or indeed volunteered their services. This is seen in banks when complex fraud or hack attack takes place. It is seen in large multi-nationals, in the breach of government services security and even in the planning of 11th September. More attention needs to be given to the value of human intelligence, where the information is collected in situ at the grass roots level.

Conclusion

Defence has always been about securing trade routes and markets. Given that Trillions of Dollars of trade is routed digitally, counter-attack electronic weapons that can disable attacking systems from other parts of the world will ultimately need to be deployed by Governments as part of their defence shield. This will save commercial operations a lot of time and money in dealing with rogue, politically motivated, electronic attacks from the rest of the world and malevolence from within which end up costing Millions in lost revenues.