mi2g

Anatomy of a Hack

An Exploration of the Effects of Asymmetric Attack

eRisk Conference – IUA Digital Risk Working Party – 30th May 2002

DK Matai - Chairman & CEO – mi2g

Introduced by David Ovenden, Chairman, IUA Digital Risk Working Party

Mr Chairman, Ladies and Gentlemen

It is a great pleasure and honour to participate in the first eRisk seminar of the Digital Risk Working Party at the IUA. Marie-Louise Rossi, the CEO of the IUA is a good friend and having been associated with the Digital Risk Working Party as a specialist advisor since its inception, I feel privileged to address such an august and diverse audience. I trust we will have a chance to learn from you and your unique experiences in dealing with digital risk during the course of this event.

The heart of digital attack lies in its asymmetric nature.

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 about 3,000 as per the new revised figures. The ratio is 1:150. 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 The sovereignty of the nation state is now being superseded by the sovereignty of the individual partly because of access to low cost travel, communications and computing power.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.

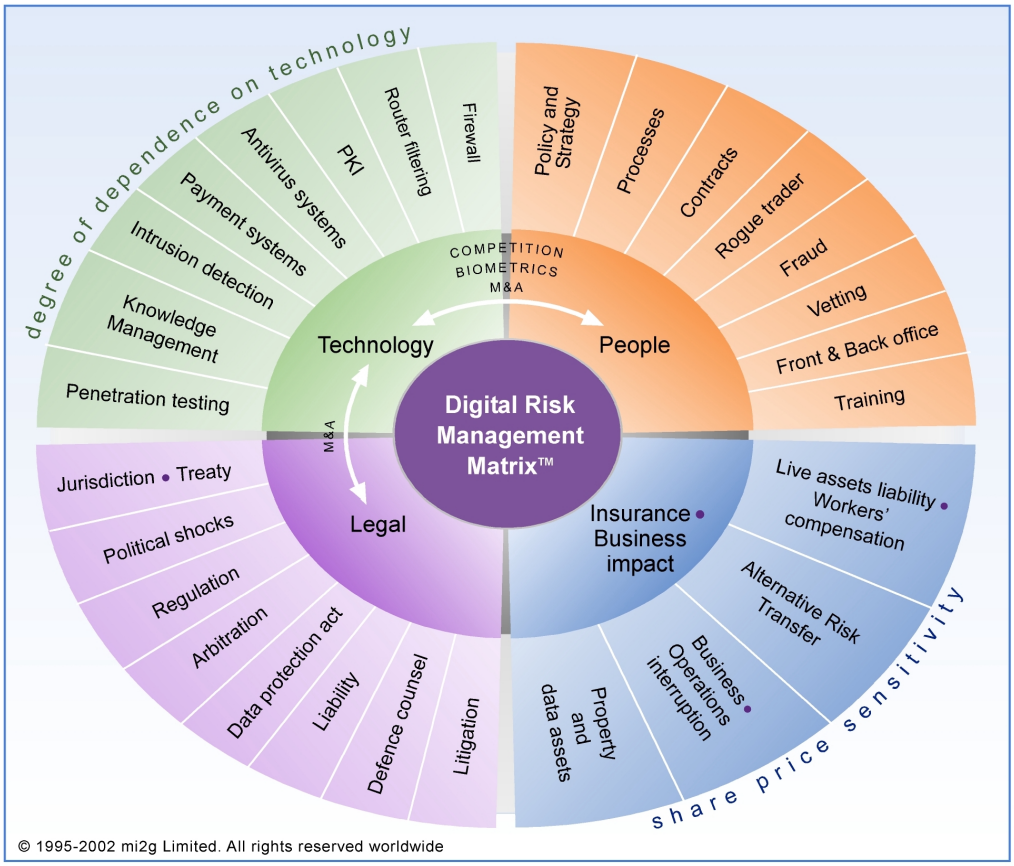
In the 21st century, asymmetric warfare is multi-dimensional. It is fought on land, on the seas, in air as well as through cyberspace.

Logic of Digital Attack

A few thoughts need to be crystallised on the logic of digital attack:

1. Our way of life in this interlinked world is more vulnerable than we acknowledge
2. Digital attack is a sophisticated activity and has to be dealt with strategically
3. Post the collapse of the Soviet Union, terrorism and digital attack continue to fill the power vacuum
4. Modern life is susceptible to digital warfare 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 and doing business

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.



Digital Risk Components

When we look at digital risk management depending on the perspective, we can see different aspects within the interlinked matrix:

1. The human resource managers see the risk as being more about people and policies as well as appropriate vetting and regular training
2. The technologists amongst you, see the risk manifest itself as software vulnerabilities, viruses, intrusion detection or system downtime
3. The legal eagles see digital risk as an issue of jurisdiction, data protection, liability and countering litigation
4. The risk managers and insurers see digital risk as essentially an issue of protecting the business via the appropriate risk transfer mechanisms

11th September has shown that digital risk management is all about dealing with the four issues - people, technology, legal and insurance issues - simultaneously.

For example:

1. Once it was clear that several hundred employees had died at one financial services group, the concern over customer service and being able to operate became one of identifying alternative personnel to do the same job.
2. Also, the main telephone lines were not functioning so Voice over IP had to be used for several days after 11th September. The dependence on corporate emails was not part of the Disaster Recovery programme for many groups, so only private eMail accounts with AOL or Yahoo were working for several weeks.

3. The mighty financial services employers also discovered that many widows did not feel that their spouses had been adequately protected and the compensation was inadequate.
4. The insurance liabilities were tightly coupled destruction of property spread into Workers' Compensation and Business Interruption.

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. This was to be expected as the estimates for the disaster rose, reaching USD 40 Billion and beyond.

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, data corruption 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. 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:

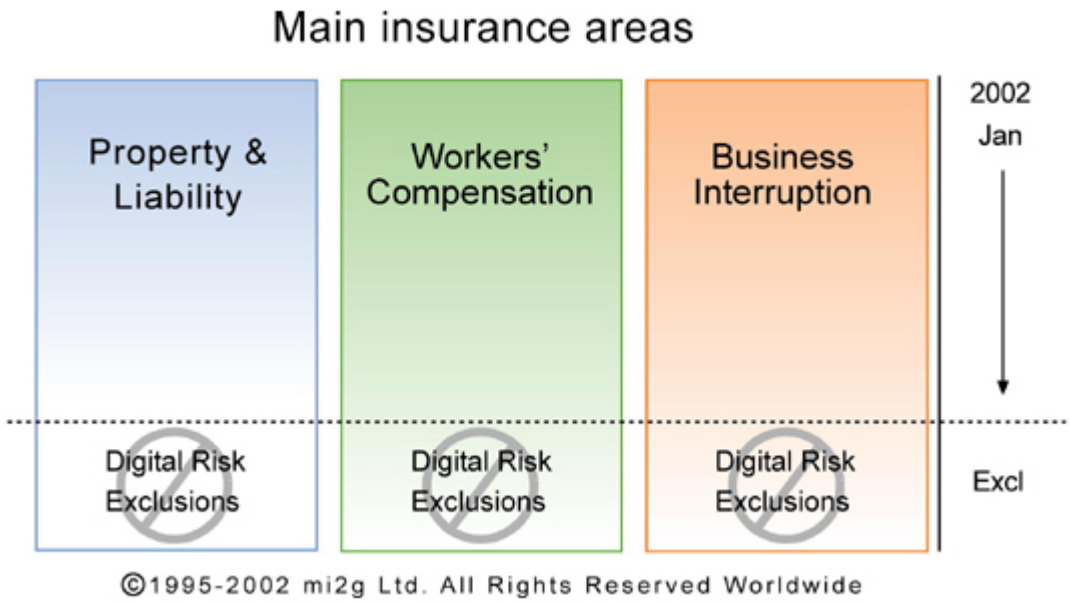
1. There is an increased demand for insurance in areas where there is less appetite to accept risks
2. Premium rates are rising dramatically
3. Policy terms and conditions have tightened significantly and now exclude digital risk
4. There is severe limiting of capacity because of man-made and natural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

Digital Risk Exclusions

As of January this year, reinsurance companies around the world have now specifically excluded data and other digital liabilities from their cover, along with terrorism. This follows warnings and announcements made in 2001.

In turn, global corporate insurers have decided to exclude data from policies to protect themselves from ruinous losses. Most businesses are unaware that digital risk exposure is in many cases no longer covered by the standard set of insurance policies, such as business interruption, workers' compensation, property and liability.

Business customers suffering from uninsured digital risks are going to opt for specialist digital risk insurance products in 2002. 11th September created massive data traffic losses for business interruption insurers. A modern corporate runs the risk of trading without having effective business interruption or disaster cover in place post the enforcement of the data exclusions. Shareholders will not accept that risk and the board will have to take some decisive steps in 2002 in this regard.



Mega-structure Risk

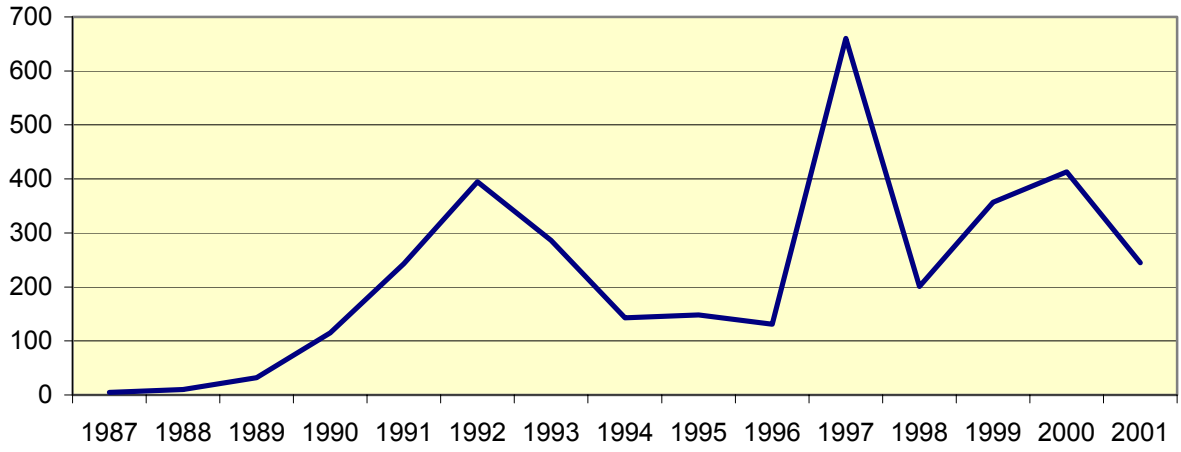
What we are facing by way of risk post 11th September is much more a mega-structure risk rather than an individualised risk. For example, if the electricity and telecom grids powering the City of London or New York fail, the business interruption is not just to one business. Several thousand organisations 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 at the conference today 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.

Software Risk

New trends are emerging with software vulnerabilities becoming the key issue over viruses in 2002. Hitherto, the building of more features has been deemed more critical to marketing and profitable sale of software in comparison to a focus on robust and zero downtime computing. All this is likely to change.

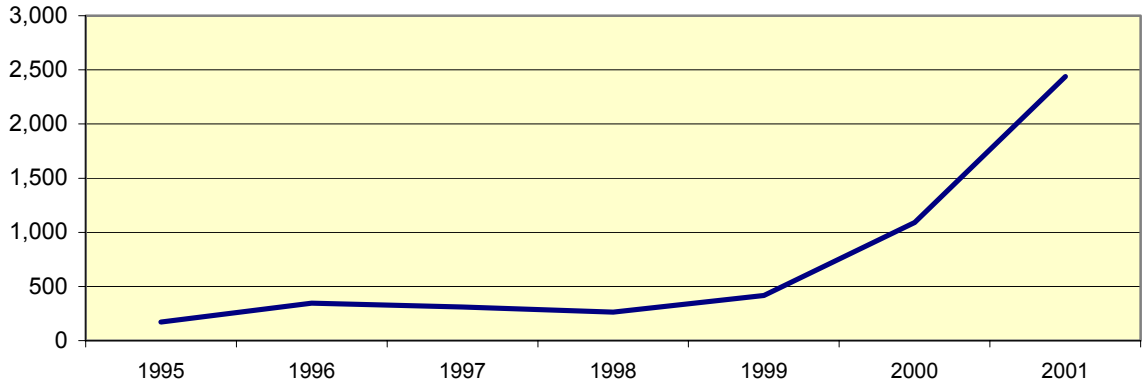
Viruses discovered per year (1987 - 2001)



The latest figures compiled by the **mi2g** Intelligence Unit show a decrease of 41% in new virus species from 413 in 2000 to 245 in 2001.

However, according to CERT, global software vulnerabilities increased by 124% from 1,090 in 2000 to 2,437 in 2001.

Vulnerabilities reported (1995 - 2001)



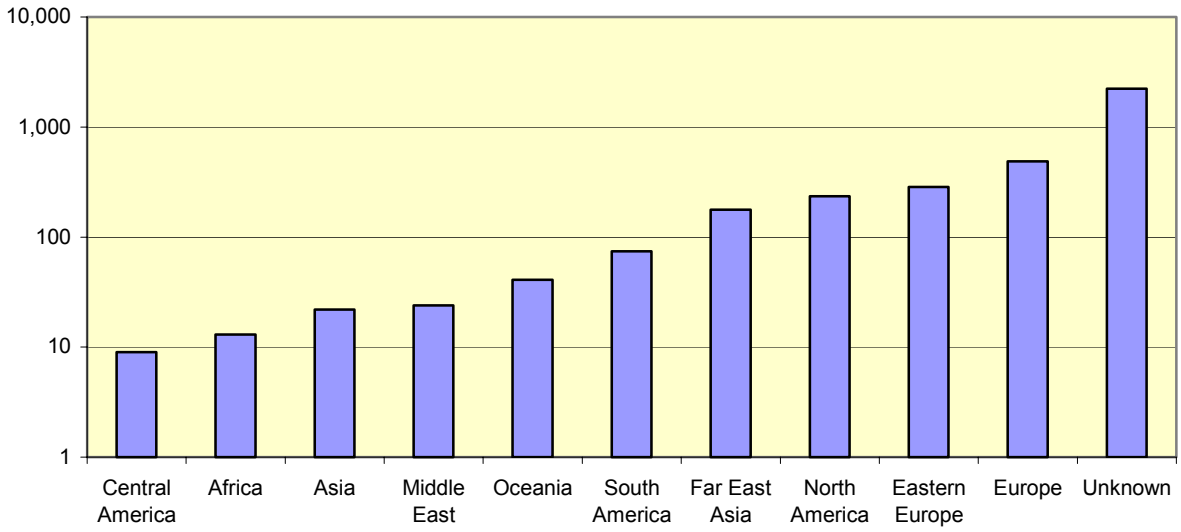
As new software vulnerabilities are exploited by virus writers, disgruntled employees and hacktivists, corporations are having to patch up their systems continuously, all of which costs time, resources and money. Carlsbad based Computer Economics institute has estimated the worldwide economic impact of malicious code attacks at US$ 13.2 Billion in 2001. The most significant attacks from internet worms exploiting vulnerabilities were Code Red ($2.62 Billion), SirCam ($1.15 Billion) and Nimda ($635 Million). In each case, Microsoft product vulnerabilities were exploited.

Microsoft's Chairman, Bill Gates sent out a memo on security to his staff on 15th January this year, which stated:

1. Microsoft must lead the industry to a whole new level of Trustworthiness in computing
2. As software has become ever more complex, independent and interconnected, Microsoft's reputation as a company has in turn become more vulnerable
3. Security models should be easy for developers to understand and build into their applications
4. So now, when we face a choice between adding features and resolving security issues, Microsoft needs to choose security

It is heartening to note that Microsoft wishes to make reliability, availability and maintainability its central theme over bells and whistles. Building Trust is a long-term issue and actions speak louder than words.

Viruses discovered by origin (1987 - 2001)



Where **mi2g** could trace and compare the origin of the virus species, Europe led the world in the development of those viruses at 57%, of which 21% originated from Eastern Europe including Russia. North America accounted for 17%, followed by the Far East at 13%.

Critical Infrastructure Intrusion

I would like to share an example of critical infrastructure breach. In October 2001, 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 Q4 last year. 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) published the code-breaking research on the web in late 2001.

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 paralysed 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?*

The new dimension of asymmetric attack is cyberspace

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

Digital Warfare'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 1990-91, 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. 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.

Digital Warfare'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 have feared an electronic attack but we have to be ready for it.

2002 CSI/FBI Computer Crime and Security Survey

On 7th April this year, the 2002 annual CSI / FBI Computer Crime and Security Survey was released. This survey is a major international news story and is very widely referenced, being a collection and analysis of data from 503 computer security practitioners. It is known for its ability to consistently challenge conventional wisdom on security issues.

The authoritative survey, in its seventh year, quotes mi2g's digital crime statistics for defacements of various international and national domains during 2001. The key take homes from this survey are:

Importance of security

The issue of digital security remains critical:

- 90% of respondents detected security breaches
- 80% acknowledged significant financial losses as a direct result
- Companies reporting security breaches rose 5% in the last five years, but the total value of losses surged from $100m to $456m

Lack of reporting

Overall, there were more computer crimes than in last year's survey. But fewer victims reported crimes to police than in 2001, reversing a trend from earlier surveys.

Specific security breaches

- Despite 89% using firewalls and 60% using IDS, 40% reported system penetration from the outside
- The use of anti-virus software by 90% of respondents did not prevent 85% from being hit by viruses, worms, etc

WWW crime

- 98% have websites and 38% suffered unauthorized access or misuse on their websites within the last twelve months
- 70% of those attacked reported vandalism, 55% reported denial of service

Biometrics

Despite having great potential when properly used, the utility of biometric authentication is often misunderstood.

- They are usually only authentication systems
- Authentication does not confer authorization; so employing biometric authentication technology does not constitute a complete security solution

The value of proprietary information

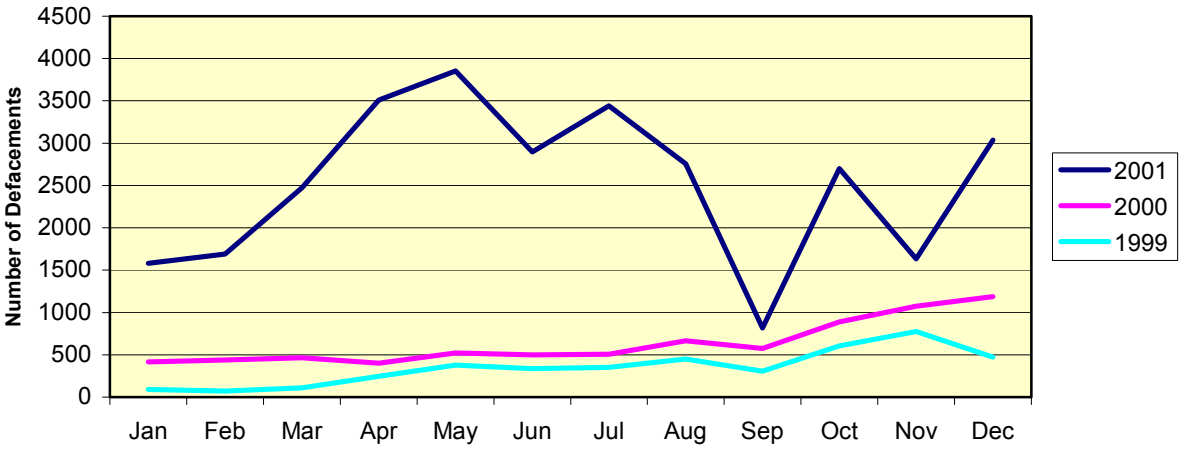
Proprietary information is one of a company's most valuable assets.

- 20% reported loss of proprietary information.
- The average financial loss due to theft of proprietary information was $6.6m, with the highest being $50m

Overt Digital Attacks

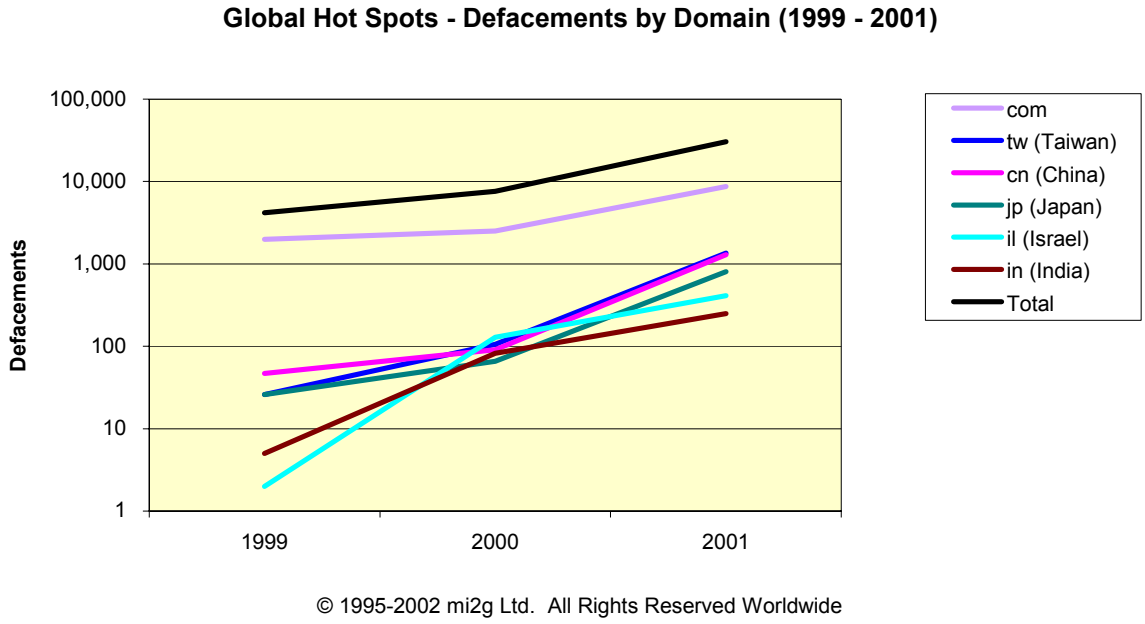
The latest figures compiled by the **mi2g** Intelligence Unit for 2001 have shown that there was a marked decrease in global web site defacements post 11th September. This could be a result of the US Department of Justice linking hacking to terrorism through the Surveillance and Anti-terrorism Bill submitted to Congress on 19th September 2001. The UK Government's Terrorism Act 2000 in which the disruption of key computer systems was classified as terrorism has also played a part in heightening awareness within the hacking community.

Web sites defaced per year (1999 - 2001)



Having said that, the number of web sites defaced globally has risen four-fold from 7,629 in 2000 to 30,388 in 2001. For example, in May 2001, there were 3,853 internet defacements world-wide whilst in September 2001 there were only 815.

Web site defacements cannot be dismissed as electronic graffiti. Between 1999 (4,195) and 2001 (30,388) this form of overt hacking has risen seven-fold. Where web site defacement has become public knowledge, in some instances there has been a significant decline in share price, loss of earnings and reputation as well as a dent in customer confidence.



Global hot-spots were echoed in cyberspace. In 2001, 63% (19,183) of all defacements of web servers were of the Microsoft Windows and Microsoft IIS combination and 18% (5,521) were attacks on the Linux with Apache combination. According to Netcraft, 63% (8,588,323) of global sites were running Apache and 26% (3,307,207) were running Microsoft in December 2001.

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 little defence capability for sustained counter-attack in cyberspace.

Digital 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 1,400 credit card numbers of forum participants, including UN Secretary General Kofi Annan, former US President Bill Clinton, Israel's Shimon Peres, 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 2000 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?

On 24th August 2001 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 reality is that 70% of all complex attacks take place through insider knowledge and assistance and not political activists who go it alone. 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. 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

1. 11th September shows that the more tightly coupled and complex our business and software systems are, the more likely it is that they will be prone to business interruption in the event of attack.

2. Good risk management and security requires the pursuit of Occam's Razor: "Things needn't be any more complex than they ought to be".

3. Open Source solutions are likely to emerge as more robust and secure alternatives to proprietary software.

4. In order to preserve business continuity, embracing distributed architecture in terms of people, technology and infrastructure is a more secure solution.

5. **mi2g**'s Guiding Principles enshrine our approach to online wealth which is:

    a. For every perceived benefit of distributed online wealth there is an associated electronic risk (eRisk). The more an online community accelerates its user traffic growth, the higher the associated eRisk.

    b. The process of distributed online wealth creation is inextricably linked to the process of online wealth protection, requiring careful frameworks to be laid out by regulatory authorities.

    c. Online wealth creation processes can be intellectual capital driven, computational power related or be subject to communications bandwidth availability.

    d. The quality of all online wealth creation processes can be measured via their effect on the reduction in response time to user needs. As the response time drops by an order of magnitude, the network effect causes the eRisk to rise by several orders of magnitude.

    e. Online wealth creation and protection processes are asymmetric. It may take several years to create online wealth and only a few seconds to lose it.