Introduction
Decision makers are not convinced that cyber threats are worth taking seriously. In part, this may be due to the apparent non-event that was the Millennium bug. This paper makes no pretence that risk assessment of cyber threats, from terrorists or others, is straightforward but aims to give a frank and objective summary of the issues.

The first anniversary of 11 September gave rise to eminent specialist groups questioning the sufficiency of US protective measures against terrorist cyber attack. The American Association for the Advancement of Science reported that the American scientific community, private sector, government and industry must all become more prepared for a cyber attack. A survey of nearly 400 IT professionals showed that over 50% thought it likely that the US would be hit by an attack in the next few months. Intelligence reporting is low volume but there has been a rise in the number of reports of terrorist groups using and being trained in electronic attack methods. The US draft National Strategy to Secure Cyberspace, published in September 2002, recognises that the number, sophistication, severity and costs of cyber attacks are increasing.

Meanwhile, Western society is now wholly dependent on electronic systems. They provide everyday services to citizens; they hold and manage all organisations’ valuable information assets; many systems are nationally critical to the delivery of electricity, fuel, water and communications. These systems are increasingly complex and interdependent – when one system fails it is almost impossible to contain the impact.

Impact
There can be little doubt about the severe potential damage that a cyber attack can deliver. These have been summarised in numerous papers, most recently in the OECD Security Guidelines published in August 2002 and will not be repeated here. Suffice it to say that electronic systems are now the lifeblood of developed Western societies. They play an essential part of almost every aspect of our daily working and social life; they are the sinews of the UK economy; they are at the heart of almost all control systems; they are vital to our military, law enforcement and emergency services. It is, nevertheless, worth emphasising some of the particular features of a cyber attack.

Critically, the impact of an attack may begin to be felt only some time after the attack has taken place. For example, viruses have been infiltrated into target systems with timing delays to cause their release some time after infiltration. An attacker may try to divert suspicion that an attack has been staged by delaying activation of a malicious malfunction.
A successful cyber attack is like the delivery of a weapon of mass destruction but without the immediate and widespread loss of life. A cyber attack against health facilities will cause loss of life even if most cyber attacks do not directly cause casualties. It is an indiscriminate form of attack because no one can tell exactly how widespread the impact of one attack will be. The widespread disruption of services will make people feel that their life support features are all under threat. The shadowy nature of a cyber attack has the capacity to create the widespread sense of demoralisation, lack of confidence in the authorities and panic in developed societies that would suit the ambitions of many of today’s terrorist groups.

This is not simply a potential threat; impacts from cyber attacks are being felt every day by organisations around the world. The manifesto of the Information Assurance Advisory Council (IAAC), launched on 16 March 2002, listed many contemporary examples. PwC calculated that US companies lost $260bn to viruses and hacking attacks in 2000. In 2001, attacks put Yahoo!, e-Bay and Amazon temporarily out of business. The 2002 DTI/PwC survey records that 44% of UK businesses suffered one malicious security breach in 2001-2002. The average cost to each business was £30,000 with some security incidents costing over £500,000. More concerning is the attempt by a security guard in 1999 to hack into a UK nuclear plant’s IT system.

Threat
The attacks of 11 September and the public rhetoric of terrorist groups associated with Osama bin Laden show intent to strike at Western societies in their totality. This is a change from the more traditional intent of IRA and other terrorist groups that have in the past eschewed mass civilian attacks. Disruption of the business and socio-political lives of Western societies seems, to Western analysts, to be an attractive vision for Bin Laden associated terrorist groups today and there is increasing mention of electronic attacks in their literature as well as in reporting of their activities. Cyber attack is a method that is well suited to non-state actors and perfect for ‘armies of irregulars’ because the ‘weapons’ are freely available.

There are different types of terrorist cyber attack: terrorists could break into a computer or communications network and introduce a new virus. Viruses take many forms and the most damaging is one that destroys data on a system and/or destroys the electronic processes that handle the data; terrorists could flood the link between an organisation and the Internet with so much e-mail traffic that the organisation’s system cannot cope and crashes; terrorists could introduce an ‘insider’ to an organisation in order to steal or tamper with information on the system; terrorists could break into a computer or communications network and surreptitiously steal or tamper with data on the system.

The tools to carry out damaging cyber attacks are readily available for would-be attackers to use. There are plenty of sites on the Internet that provide the tools for easy download. There are also a large number of discussion groups and other ‘chat rooms’ where attacking expertise and knowledge is shared and developed. An expert user of everyday computer or communications equipment would have sufficient expertise for some types of attack, attacking websites for example. Many sites have poor password protection, or non at all, allowing an attacker to enter easily and deface the site with obscenities, divert subsequent visitors to a site of his choosing and/or create a new vulnerability to future virus attacks. These straightforward attacks are damaging to reputation and costly in terms of lost business.

Specialist skills would be needed, however, to carry out a surreptitious attack without risking revealing the attack to the system owner. Terrorist groups will be capable of hiring, recruiting or blackmailing people with the skills and experience to undertake highly damaging cyber attacks. They will be most likely to obtain these people through organised criminal groups who have developed cyber attack capabilities. Some groups have the resources and the incentive to invest in high quality collaborators and to train them well. Many of these
Almost all information systems in business and public use are highly dependent on others. For example, in early 2002 a breakdown in a major piece of BT equipment in Hampshire was followed by the failure of a power back-up system and resulted in the total failure of the emergency 999 systems in some areas. Not only is there a huge number of mutual dependencies between systems, but also there is little information about these dependencies. The fuel crisis, albeit not primarily an information system crisis, showed vividly that dependencies almost invariably take the emergency response managers by surprise.

Many large companies, government departments and major service providers outsource many of the business and technical services to third parties. These arrangements create a number of dependencies on the outsourcing provider. And a successful terrorist cyber attack on a third party supplier will impact on a number of their customers. Outsourcing will remain a feature of the IT industry and the relationships involved need to take more account of security issues than they do at present.

**Vulnerabilities**

Vulnerabilities in systems and in software correlate with the level and type of threat to systems. Threats follow vulnerabilities much more in this cyber threat area than in other threat scenarios. News of a potential weakness in a software package spreads rapidly to system administrators all over the world to alert them to the problem and it is inevitable that people in the hacking communities learn about it as well. Furthermore, hackers put great efforts into probing software packages for weaknesses and may well discover a weakness that the manufacturers and the user communities have yet to find. Once a weakness has been found, it is common for cyber attackers to probe all the instances of a particular software or system in the search for an opportunity to exploit it. Scanning a vast number of potential victims is so much easier electronically than in other potential attack situations.

Information systems are highly complex entities comprising many separate elements. The complexity makes it difficult to judge whether the system is working satisfactorily and is undamaged; it is surprisingly hard to be confident that a system is in a normal and/or good working condition. This makes early detection of the attack difficult. Major crashes and defects are all too obvious but most systems in organisations have functionalities that are not in regular use by the organisation’s staff. A system defect or some forms of attack might remain unnoticed for some time in rarely used parts of a system.

Marketing pressures encourage the rapid production of new software and upgrades of existing packages. Costly quality control and security features often take second place to market pressures for quick production and low cost products and many defects may still exist in the software products; there were thousands of defects in Windows 2000 when it was first introduced. These are often found first by the hacking community who commit time and energy to finding ways to exploit these vulnerabilities.

Almost all information systems in business and public use are highly dependent on others. For example, in early 2002 a breakdown in a major piece of BT equipment in Hampshire was followed by the failure of a power back-up system and resulted in the total failure of the emergency 999 systems in some areas. Not only is there a huge number of mutual dependencies between systems, but also there is little information about these dependencies. The fuel crisis, albeit not primarily an information system crisis, showed vividly that dependencies almost invariably take the emergency response managers by surprise.

Many large companies, government departments and major service providers outsource many of the business and technical services to third parties. These arrangements create a number of 'many-to-many' relationships. A successful terrorist ‘hit’ on one organisation immediately increases the risk of a subsequent cyber attack on another supported by the same outsourcing provider. And a successful terrorist cyber attack on a third party supplier will impact on a number of their customers. Outsourcing will remain a feature of the IT industry and the relationships involved need to take more account of security issues than they do at present.

**Risk**

It is both easy to over-hype the threat and to underestimate the likelihood of an attack taking place. Much of the media and some security product manufacturers tend to exaggerate the cyber attack threat; conversely, many organisations appear to assume that only other people or organisations will be targets of cyber attacks – it will not be them. We know that cyber attack tools with a potentially highly damaging impact do exist but there is no clear way of predicting the likelihood of them being used.

Even though it is hard to measure, the consensus amongst expert and academic analysts is that the risk is serious and should be taken seriously. The level of government activity supports this judgement.
The risk of a terrorist cyber attack should, therefore, be included in all organisations’ risk assessments.

Obstacles to effective response
Managing the risks posed by cyber threats is a complex matter. No single organisation can achieve this alone. A high degree of cooperation and co-ordinated responsive actions by a wide range of organisations is needed to achieve significant protection against this threat. Many senior managers and board directors are anxious about making decisions involving information systems. These systems represent major investments for organisations and the issues involved in these decisions often feel alien to many of the would-be decision makers. The 2002 DTI/PwC survey reported an increase from 53% (in 2000) to 73% of businesses believing that information security is a high priority for senior management. But few of the decision makers have competence in these matters and even fewer still have experience of handling security or safety issues as corporate matters. The language involved in information systems inhibits easy communication of risks between corporate decision makers and specialist staff, consultants and product vendors.

Most organisations are reluctant to give information about attacks and, even more so, about the degree or amount of damage inflicted on them. A recent UK attempt to establish a prototype Information Sharing and Analysis Centre (ISAC) within the IT communications sector has failed. In spite of creating a secure and trusted environment, members of the industry turned out to be unwilling to commit themselves to sharing information.

It is also difficult to provide boards with a convincing business case for investment in protective measures. There is a negative feel to security in that it seems to cost money but does not necessarily provide business benefits. Specialists in the field are confident that good information security brings potential competitive advantage but they do not succeed in convincing many at board level.

Some ways forward
Conference speakers and academic papers have been saying for a few years that managing the risks from cyber threats requires a coherent, co-ordinated and joined-up approach from public, private and not-for-profit sectors. Regrettably, very little substantial progress has been made to make tangible and practical progress on this.

The possibility of a severe cyber attack has prompted most Western and other governments to invest in protecting critical national infrastructures (CNI). States have sought to identify the electronics systems on which their whole nation depends and endeavour to find ways to increase the protection afforded to these systems.

The UK’s National Infrastructure Security Co-ordination Centre (NISCC) was founded in 1999 to take forward this work. Their work has led to identification of the UK’s critical infrastructure and establishment of security standards necessary to provide protection against the prevailing threats. The National Hi-Tech Crime Unit (NHTCU) was established in 2001 to be a focus of law enforcement work against cyber crime. NHTCU is both a centre of investigative excellence and a support to all police forces in England and Wales for their work against computer crime. The Office of the e-Envoy (OeE) was appointed in May 2002 to lead and sponsor all the Government’s work on the protection of information and data systems from cyber attack. This is a valuable development.

But much more needs to be done. The OeE is working on a UK strategy for information assurance; this product is needed as soon as possible for two main reasons. Firstly, there is lack of clarity about the roles of the numerous government agencies because their remits overlap. Their functions are clearly defined and are fine in theory, but when engaging with UK industries, businesses and the citizen, their roles become very confusing. In addition, each of the public bodies have to put resources into harmonising their various activities and these resources could be better used directly confronting the problems of risk.
Part of the information assurance must be to build a real and effective community of interest involving all the public bodies associated with this work. A committed sense of shared endeavour is needed to change the public sector culture of cutting up the business between departments and then defending each piece of ‘turf’. One of the many tools needed is a shared information environment where all public sector organisations involved in cyber threat protection can share information within the constraints of each one’s privacy and security regimes. Such a system is being developed for the anti-fraud community using the UK Government’s ‘Invest to Save’ funds and could be applied to the information assurance business too.

Secondly, the strategy is needed to provide urgent impetus to bringing much more effective joint working between UK public bodies, not-for-profit organisations and the private sector. Most recognise the need, in theory, to work together but meetings are laced with a sense of wariness and few people attempt to overcome the first hurdle of talking a common language. Public bodies put a high priority on processes while the private sector focuses on outcomes. Both approaches are valid in their own way but what is needed is a commitment to working together to achieve practical benefits.

The private sector businesses and industries must also show stronger commitment to joint working. A good example of where this approach is needed is in the manufacture of secure software products. There is little market incentive for vendors to build in high levels of quality or security features to their software products (for reasons that have been touched on earlier in this paper), but it is not in the national interest for the software industry to continue to produce products that are shot through with defects. Easily said but much harder to tackle; an integrated and holistic initiative by government in partnership with the private sector is an essential factor for success.

The private sector is not making best use of the existing resources because their response to this threat is too segmented. Industries and businesses tackle the risk as they think it affects them individually and do not recognise that the dependencies between systems and organisations are so extensive that they need to work much more together in responding to this threat. Industries and businesses are locked into silos, communicate little and work together only occasionally. There are excellent initiatives by the CBI, IoD and others but these are covering only a tiny minority of the organisations that need to take a much more active role in tackling this threat in a shared way.

One of the most important initiatives is information sharing, where a group of organisations or individuals enter into an arrangement to share information for the good of the group. This has to be a highly trusted sharing process because much of the valuable information will involve embarrassing and potentially damaging knowledge about one of the participants. For example, businesses or companies will only be prepared to share information for the good of a group if they can be certain that the information will not leak out and damage reputation, sales or share value.

There are a growing number of such sharing entities in the US but, as mentioned earlier, the first prototype in the UK has failed. Large sections of the US private sector have recognised, albeit after a few years of pressure from Washington, that sharing information is much more likely to achieve individual and corporate greater good than hiding it. There are some UK initiatives for information sharing but much more commitment and support from the UK government and the private sector is needed.

NISCC is promoting Warning and Reporting Points (WARPS) as a particular way of establishing the necessary organisation for information sharing. IAAC has been pushing the concept of information sharing too. In 2001, IAAC completed a study that argued the benefits of sharing threat and early warning information. The annex to the paper contained analysis of the benefits and disadvantages of about 20 different information-sharing models that have been tried.
Information sharing has particular relevance in a counter-terrorist context. It can be described as a market differentiator for potential targets of terrorist cyber attack. In most situations, terrorists work in secret and in compartmentalised cells – to avoid the globe’s major intelligence organisations who are hunting for them. This can give their targets a marginal advantage by developing communication networks to provide early warning of attacks; by being well informed about the cyber terrorist threat and by sharing information about actual attacks.

Yet, information sharing is a significant challenge for the way Western businesses and citizens normally behave. The marketing of products relies to a large extent on competing organisations ‘talking-up’ the quality of their products through advertising and other means. Information about problems, shortcomings and crises is withheld because of the damage it could do to an organisation’s prospects. This market-driven urge for confidentiality is the greatest weakness of Western organisations that face cyber threats. Terrorist groups and other cyber attackers continue to have opportunities to attack because most potential targets are building protection in isolation.

There are many dependencies between organisations and it is just as much in the interests of the yet-to-be-victimised organisations as it is for those already damaged to encourage information sharing to reduce each organisation’s vulnerabilities to future attacks.

**Conclusion**

The terrible events of 11 September have justly focused security managers’ attention on further measures to reduce the risk to people. Just over one year on, businesses, citizens and security professionals should be encouraged to look afresh at the types of threats they face. We all need to move our attention away from focusing solely on the last threat to predicting the future sources of terrorist damage to people, property and ways of life.

The thrust of this chapter is intended to be a challenge to an accepted way of Western working hidebound by confidentiality. If companies and governments do not rise to this challenge they will miss their main advantage over the cyber terrorist: their ability, collectively, to be smarter than the attacker. Sensible defences can only be achieved through developing trusted sharing practices and other ways of working together on threats and vulnerabilities. Successful protection in the face of what looks like an increasing threat of cyber terrorist attack needs much more imagination, collaboration and energy on information assurance than is today’s norm.

---

1 “Information Security Breaches 2002” available at
2 www.alldas.org