Bad blood

With online fraud now worth more than £50bn a year worldwide, cash-strapped governments are still making new resources available for cyber security, reports Graham Buck

As the end of the first decade of the 21st century approaches, terrorism still ranks high on the global risk agenda. But online fraud and cyber security now rival it as a serious concern for most world leaders.

The ability of cyber attackers to create mayhem was demonstrated early in July. South Korea and the US fell victim to attacks that involved sending multiple requests for website access from 166,000 'zombie' computers in 74 different countries. US government sites that were briefly knocked out included the State Department, The Federal Trade Commission, the Homeland Security Department and the Federal Aviation Administration, while the New York Stock Exchange, the Nasdaq electronic exchange and the Washington Post were also hit.

Despite initial reports suggesting that North Korea was behind the attacks, it transpired that they could have been launched from a master company belonging to an internet television company in Brighton.

The business world also has cause for alarm at the increasingly audacious attacks on its online systems. Although banks are regarded as being prime targets, retail sites have been hit the most. Perhaps the most spectacular was the theft of information from over 45 million credit cards from US retail giant TJX (parent of T K Maxx) by hackers who breached the group's computer transaction processing systems from July 2005. Their attack continued for 18 months before being detected and is estimated to have cost the group as much as US$80 million.

Other retail victims include BJ's Wholesale Club, Boston Market, Barnes & Noble, DSW, Forever 21, Sports Authority and OfficeMax, says Toyin Adelakun, senior security consultant for SunGard Availability Services – and these are just the ones that have been made public.

Whereas the typical hacker was once a teenage 'geek' operating from his bedroom, sophisticated gangs of online criminals now target sites. DarkMarket, Golden Cash and other rings are recognised to have been set up as "firms", with distinct business models and existing along identifiable value chains, reports Adelakun.

Members and leaders of organised gangs have been apprehended in countries as far apart as the US, Turkey, New Zealand and Romania. One Romanian gang leader was tracked to the home of an elected politician that suggested a degree of inter-governmental cooperation on cybercrime, while the TJX attack was attributed to a Ukrainian code-named 'Maksik' based in Turkey.

The hierarchical nature of these "firms" means no single profile fits all hackers, says Adelakun. They range from technical wizards who create hacking exploits and overlords who plot strategies to mere "clickers" who just run point-and-click tools and endless participants with varying degrees of technical nous and seniority and connectedness. As he observes "the one thing that the impecunious teenager in Romania will have in common with the contact-centre jockey in India and the wily technician in New Zealand is a desire for more money."

Historic precedents

The degree of organisation behind these attacks has moved cyber security firmly to centre stage. "At a time of global financial crisis, when so many demands are already being made on the public purse, it is remarkable that both the US and UK governments are committing significant new resources together with new national approaches to cyber security," comments Stuart Anderson, resilience specialist for PA Consulting Group.

In late June the UK government announced plans to set up a new Office of Cyber Security (OCS) to provide "strategic leadership and coherence" as part of a comprehensive effort to protect Britain's IT structures. The OCS will draw on the expertise of individuals from the Ministry of Defence, the UK's intelligence services and law enforcement agencies.

Also being established is a multi-agency Cyber Security Operations Centre to bring together activities such as monitoring cyberspace, assessing attacks and breaches, co-ordinating responses and advising both the general public and the business world on cyber security risks.

The announcement came only a few weeks after the Obama administration unveiled its own cyber security initiatives, demonstrating that cash-strapped governments on both sides of the Atlantic can still muster funds to address a problem.

Gordon Brown even drew on historic precedents as he declared: "Just as in the 19th century we had to secure the seas for our national safety and prosperity, and in the 20th century we had to secure the air, in the 21st century we have to secure our position in cyberspace in order to give people and businesses the confidence they need to operate safely there."

A Home Office report *Extending our reach: a comprehensive approach to tackling serious organised crime* pledges to step up efforts to combat online fraud and cyber crime. As commentators noted, this amounted to a tacit admission that earlier problems have failed to make much impact on the problem. The UK is not alone in its failure though, with online fraud worldwide now estimated to be running at more than £50bn a year.

The report states that central to developing a stronger response to cyber crime will be the £7.4m police central e-crime unit that was set up last year in response to lobbying by the police and business.

The underlying message in the National Cyber Security Strategy is that organisations need to improve their ability to understand and mitigate risk from the use of cyber space, says Anderson. Many businesses are already dealing with these threats; what has changed is that the strategy officially gives notice that the legal and regulatory framework will be tougher.

"Better management of risk will afford early adopters the chance to gain competitive advantage and increased shareholder value," he adds. "This all strengthens the case for maintaining IT security budgets during the downturn to combat the growing threat of cyber crime in all its forms, even though overall IT budgets are under extreme pressure."

Anderson says that IT security typically accounts for six per cent to eight per cent of an organisation's total IT budget, while those that address the human factor (reducing fraud and other insider threats) will spend around an additional three per cent for an effective audit and initial response capability.

Rising to the challenge

The new initiatives mark the first major concerted efforts on cyber security since the late 1990s, says Neil Fisher, vice-president for identity management at Unisys. At that time the US, which has traditionally led the way on policy, launched initiatives PDD63 and PDD62 led by Security Affairs National Coordinator Dick Clarke and 'security czar' Howard Schmidt and established the National Infrastructure Protection Center. They were good ideas and good institutions, but their efforts were undermined by power plays at the top level and the dominance of the FBI.

In the UK, there was considerable difficulty in finding a politician willing to take on the challenge and the remit ended up with the Home Office, which established the National Infrastructure Security Coordination Centre (NISCC) – now the Centre for the Protection of National Infrastructure – housed in MI5. While NISCC has enjoyed a good relationship with industry, Fisher suggests its tendency has been to issue warnings to companies at regular intervals rather than actually take action.

Since 2006, the Serious Organised Crime Agency (SOCA) has merged the activities on several UK anti-crime bodies and, says Fisher, has grown accomplished in tackling sophisticated and complex cybercrime – particularly attacks on banks, which can involve criminals in numerous EU countries pooling their efforts to form a sophisticated gang. And larger organisations have been able to build up their cyber mitigation strategies.

By contrast, the government's own departments have proved fairly inept – demonstrated most notoriously in November 2007 when the head of HM Revenue and Customs resigned after CDS bearing the personal details of 25 million Britons were lost in transit.

The creation of the OCS is a signal that the government is responding to the changing nature and scale of cyber crime and this is likely to be reflected in a more stringent legal and regulatory framework, says Anderson.

Much of the impetus has been the increase in state-sponsored cyber attacks says Matthew Norris, manager for Hiscox Technology. Of particular concern are attacks against government sites emanating from China, which have a history of attempts to steal data from major Western powers.

Norris notes that liaison between the UK and the US has been stepped up over the past six months. "Both were previously working in isolation, then realised that the attacks were broader and more sophisticated than they had previously imagined."

Russia also demonstrated its capabilities last August in the conflict with Georgia, when its physical attacks were accompanied by coordinated and concerted cyber attacks. Extortion is a further aspect of cyber crime giving rise to concern. For example, motivated by political or ideological motives, gangs may threaten or attempt to shut off key aspects of public infrastructure. A local airport in

the US suffered the loss of its electricity supply last year after a cyber attack.

Add to these incentives a desire to "protect UK plc", says Andrew Wilson, who heads the information security practice at PricewaterhouseCoopers. The OCS strategy aims at defending the British economy. While large companies are not immune to risk and must keep abreast of new threats they have developed cyber security strategies and mechanisms. In addition, their risk professionals network extensively with those from other major organisations to pool their expertise and experiences.

However, SMEs lack the resources and the track record necessary to successfully manage their online operations says Wilson. This means that if security breaches continue to escalate they could ultimately result in their online operations representing "more of a threat than a benefit".

Norris cites one example; major retailers are generally permitted a rate of up to five per cent as a percentage of fraudulent credit card transactions to genuine ones. If this threshold is exceeded, the Payment Cards Industry (PCI) will take action and also impose a hefty surcharge for the use of the card(s) that break the limit. "This can really pinch a company hard and is far more worrying for a company than any UK government action," he adds.

Outside the comfort zone

How should risk managers respond to these new challenges? Fisher suggests that their strategy should be to take advantage of all opportunities to share information with their peers.

"Digital Britain is full of marvellous visions, but the company must still be mindful of its duty of care when dealing with customers and clients. So risk managers should develop a rapport with the OCS and SOCA to ensure they are up to date with techniques and that they share their experiences with the government," he recommends.

"They should be extremely vigilant and extend their responsibilities with the chief executive and the board. This means proper investment in the company's infrastructure. Admittedly it's a hard task during a recession, when companies may be in the midst of restructuring and also reviewing the option of cloud computing."

The risk officer must also be on the lookout for potential insiders, which means "asking how well you know your staff and whether you are familiar with their roles and responsibilities." This will entail logging desktop activity to check whether individuals are following company policy on cyber security – and also whether they are engaged in legitimate activity or simply looking at Facebook.

Fisher also recommends the site www.sonicwall.com/phishing which offers then examples of e-mails, some of which are from a genuine site while the others are 'phished'. Users are invited to distinguish the genuine messages from the fraudulent ones and less then one in ten individuals score 100 per cent on the test (indeed, this writer only managed 60 per cent).

For IT security professionals, the task is to provide expert leadership that helps senior management prepare their organisations for this new risk landscape, says Anderson.

So in addition to ensuring that fundamental security standards such as ISO27001 are well covered, they must ensure that the organisation adopts a demonstrably effective approach to managing risks.

"This may mean stepping outside their comfort zones to help senior management manage risks across the organisation. It may mean reminding senior management of basic principles of good systems development and programme management – and reflecting these explicitly in risk registers," adds Anderson.

"The best IT security professionals already do this.
In short, IT security professionals have an opportunity to widen their organisational reach, doing what they already do well but across boundaries that have traditionally been difficult to cross."

Wilson adds that one of the OCS's main tasks is to ensure that SMEs can leverage the advice of security professionals. Those working for major organisations have seen new challenges regularly arise and developed the skills needed to tackle them.

"So the need is to turn the wealth of expertise out there into good practical information that SMEs can make use of," he says. "Obviously this should have been done sooner, preferably during the boom times, but developments are notoriously not governed by logic.

"Lastly, companies that carry out cost to benefit analysis of installing online security measures should remember that in the current climate if they lose their reputation as well then they are really sunk," says Norris. One positive development has been a steady decrease in the cost of security, so that measures such as encryption – initially very expensive and complex – have become significantly cheaper.