Cyber Assault
By Michelle Price
Information Age, April 2007
http://www.information-age.com/article/2007/april_2007/cyber_assault

The threat to the UK's critical IT infrastructure from cyber terrorists, activists and others with serious malicious intent is very real and growing.

Not long before Christmas 2006, Gus Cunningham's phone began ringing off the hook. Rather than seasonal greetings, he was confronted by the anxious tones of security chiefs from some of the world's largest financial services organisations, all of whom had just received a warning from the US Department of Homeland Security of a potential, terrorist cyber-attack on Wall Street's trading systems. "The calls started on the Friday," he recalls, "and by Monday afternoon I had been to financial institution after institution, trying to answer one critical question: 'Are we at risk?'"

A false alarm on this occasion, the incident nonetheless reverberated across the finance world, with companies eager to close down their exposure to some of the highlighted threats, such as a largescale denial of service attack, an area where Cunningham's company Prolexic Technologies offers a protection service. Cunningham, Prolexic's UK managing director, freely admits that such scares are good for business, but the risks are real, he argues, and they are growing. Most banks, he claims, "could not handle even a simple cyber attack" – and they are far from unique.

As the case of Gary McKinnon, the UK hacker facing trial for allegedly breaking into 97 US military and Nasa computers, has highlighted, even vital IT systems relating to defence and government are highly vulnerable to patient, determined attack. For this reason, several major law enforcement organisations – including the Serious Organised Crime Agency (SOCA), Scotland Yard and the FBI – have recently turned their attention to cyber-assaults, in the belief that these activities pose a significant threat to the critical national infrastructure (CNI) and global business in general.

Indeed, with nearly 90% of the CNI privately controlled, points out Phyllis Schneck, chair of InfraGard, the FBI-run IT security programme, cyber-terror is just as much, if not more of a threat to the corporate community, as it is to governments and civilians.

And that threat continues to grow, as global communication networks and information systems become increasingly interconnected.

Currently, says David Lacey, former head of IT security at both the Royal Mail and Shell, and founding member of security association the Jericho Forum, global information systems are experiencing a "critical convergence period", in which growing Internet connectivity, a loss of perimeter security and the increased vulnerability of platforms are forming a precarious conjunction.

Consequently, systems governing key operations – relating to finance, utilities, oil and gas, supply chains, healthcare and transportation – that were once secure when operated discretely, have lost much of their robustness after being joined together. This has created a raft of hidden dependencies, the critical nature of which was underlined in 2003, reports the US National Infrastructure Advisory Council (NIAC), when the release of the Sobig virus temporarily caused the suspension of 23,000 miles of one US railway system and, separately, cut Air Canada's phone-reservation capacity in half.

Educated enemy

As such vulnerabilities continue to multiply, there remains no shortage of individuals and groups willing and, more importantly, able to target and exploit them. Far from languishing on the technical fringe, terrorists and activists are highly adaptable, says Dr Andrew Colarik, an expert on cyber-warfare and co-author of the recently published Cyber Warfare and Cyber Terrorism. As a result, there is a growing body of evidence to suggest that the technical expertise of such groups is now dangerously mature.

Some activists and terrorist groups, including Al Qaeda, Hamas, Hizbullah and white supremacist organisations, have proved their technical capability in the past in documented incidents involving the remote opening of a dam and the disruption of power services. Nearly all have perpetrated hacking attacks of varying extremes, the victims of which have included Visa, the Israeli Central Bank, the Tel Aviv Stock Exchange, AT&T, and Lebanese television services. In one incident reported by the US National Criminal Investigation Service, pro-Palestinian activists succeeded in paralysing half of Israel's entire email network for several days.

Assaults of this nature are considerably less costly to conduct than those methods used to perpetrate physical attacks, while the necessary resources can also be easily obtained and reused. Disruptions, as the last example proves, can also be sustained over a long period of time, and executed from remote locations.

And there is more to come, warn security experts. They talk of the perpetration of a large-scale 'joined up' cyber-assault, designed to exploit vulnerabilities in global infrastructures. This vision, says John Walker, vice president of the Information Security Systems Association (ISSA), and chief security officer at a major financial services company, is not the far-fetched stuff of security technology suppliers' fantasies.

"No-one predicted an event of the scale and organisation seen on 9/11, but it happened nonetheless. It is therefore feasible that something could happen on that scale in the cyber world, via the Internet," he observes. Such an eventuality, asserts InfraGard's Schneck, "is not a matter of if, it's a matter of when", and that 'when', agree both Walker and Lacey, is likely to be within the next two years.

If the corporate community is to arm itself against such an attack, it will have to carefully map its IT infrastructures in order to trace unknown vulnerabilities. This will also involve revisiting aged legacy systems, says Schneck, and building in security measures and redundancy retrospectively. Above all, she stresses, the business community must learn to build "trusted relationships", in order to share expertise across both cyber and social networks.

Hacktivism

While the business community must move to harden its electronic defences against a large-scale assault aiming to exploit convergent dependencies, individual businesses should also be prepared to defend themselves against discrete, targeted attacks perpetrated by activists, organised criminals and, in some cases, terrorists. According to research by unified threat management provider Webroot, this security issue is among the most pressing for the corporate community, of which a staggering 43% currently suffer some form of systems disruption as a result of targeted malware.

In many instances, malware attacks result in the corruption or leakage of corporate data, which is then exploited for a variety of purposes, more often than not, financial. But other tactics deployed by criminals and cyber activists (or 'hacktivists', as they are self-named) can prove far more aggressive, including the defacing of websites, vandalising or deleting of files, reconfiguring passwords, rerouting connections to counterfeit websites, public distribution of private information, email flooding, domain name server attacks, or a full scale denial of service attack.

For organisations with an extensive online presence, these latter forms of cyber-assault can prove singularly devastating, and they are regularly deployed for the purposes of both criminal extortion and to promote political goals. As the security officer at a major broadcaster reveals, his company is frequently the victim of cyber protests, executed across its several hundred web portals. In particular, the organisation's annual awards have repeatedly been targeted by anarchist groups attempting to manipulate the outcome by falsifying competition votes.

"Typically we have discovered this problem through focused voting: a particular ISP in a particular country suddenly starts pouring votes onto the site. As soon as we move to block them we become open to more aggressive attacks, including distributed denial of service (DDOS), and email bombing – which is one of our major issues."

In addition, he continues, anti-globalisation and anti-capitalism groups regularly try to deface the organisation's websites, which at the very least can prove time-consuming to correct, and at the worst highly damaging to the company's well-established brand.

Misuse and disruption of hacked data also remains a constant concern for such organisations, especially those that hold vast banks of private and extremely sensitive information. For the Royal College of Physicians, for example, protecting its database of doctors' personal information is a "key worry", admits Christopher Venning, IT network manager at the association. "Anti-abortionist and anti-vivisectionist extremists would like to get hold of home addresses, and we are aware that other colleges have been targets of hacking attacks for this purpose."

Nearly all central government websites, aerospace companies and defence environments, including NASA, are major and frequent targets of such focused information hacks, reveals a security officer at a chemicals manufacturer, the perpetrators of which are usually foreign intelligence agencies. State sponsored cyber assaults of this kind are among the chief concerns of the Ministry of Defence, Information Age has learnt, with the UK now exposed to more than 40 hostile countries that regularly attempt to penetrate both corporate and government IT networks.

Self-defence

Defending against determined attackers remains a complex and costly challenge, and one that requires a good deal of imagination too. Among the most basic business processes that should first be addressed, however, is information lifecycle management: ensuring that the organisation's assets are protected in order of priority is a good start, says David Emm, senior technology consultant at anti-virus specialist Kaspersky Labs.

A battery of technologies should then be wrapped around these assets, he continues, including a firewall at either the gateway, or the desktop to guard against botnet activity; anti-spam capability to prevent the proliferation of Trojans; and anti-virus software, which itself should include behavioural analysis and intrusion protection, in order to detect exploits and hacking activities. Up-to-date patching is also crucial, he adds.

Moving from simple anti-virus software to a full anti-malware set, however, can prove difficult to properly execute within large organisations, due to the amount of computer power involved, observes the chief security officer of a FT 100 company. "To analyse everything in-house would basically stop the end user from operating, so it's not possible to attempt everything at the desktop. This often means moving to a managed service provider" – an increasingly prevalent security strategy, that often saves resources in the long term.

It is the human factor, however, to which security specialists repeatedly return. In the case of cyber terror, assault and crime, the most critical long-term measure is to work with the authorities, says ISSA's Walker. Currently, it is estimated by InfoSecurity Europe that at least a third of victim organisations fail to report incidents to the authorities, thereby depriving law enforcement agencies of valuable cyber-intelligence. Only by plugging this gap, and exposing the true scale of cyber assault, can the corporate community hope to establish a successful, long-term self-defence.

In denial

DENIAL of service mitigation company Prolexic protects a range of online forums and websites, the content of which "not everyone necessarily agrees with", explains Gus Cunningham, its UK managing director. These include Tomaar, a Saudi-based liberal rights online organisation and CastleCops, an online security forum, both of which have repeatedly been victims of distributed denial of service (DDOS) attacks.

In the case of Tomaar, reveals Cunningham, Islamist radicals have attempted to entirely disable the site while the Saudi government has frequently blocked it. CastleCops, which services a range of prize brands through its web presence, is subject to regular "very damaging" attack by criminals and Internet activists, says Paul Laudanski, the site's founder.

The latest of these attacks occurred on Valentine's Day 2007, reveals Laudanski, in the form of a multi-pronged assault of five separate high surges of traffic, beginning at a little under a gigabit per second and lasting for up to one hour. "The attacks saturated the entire network. Nobody knew about or expected something like this to happen, so it caught everybody off guard," he recalls.

Using a botnet, the attackers deployed two techniques: the first, Laudanksi explains, was the use of "'http gets', by which the botnet makes requests to a certain location of the site." The second involved a range of data floods, including UDP, TCP and SYN floods. "Originally it looked like the DDOS was coming at us from our domain, and it quickly switched over to IP, so by the second surge they started attacking our domain name server (DNS) as well," says Laudanksi.

At this point, CastleCops was forced to move its DNS reference points to Prolexic's IP space, which is Prolexic's principle method of DDOS mitigation. "Once the attackers realised that our DNS was no longer at that current location and moved off to Prolexic, they stopped attacking our DNS and went straight to IP," Laudanksi continues. "At that point we had to leave that location, because our ISP couldn't handle or mitigate that kind of attack."

Since moving to a new ISP, CastleCops has been able to absorb further DDOS attacks, all of which Laudanski reports to the authorities. Retaliation, he adds, is not an option. "The most important message is that you cannot retaliate, not only because you are then joining their ranks, but because you will only retaliate against botnet victims."