The access Code to the Netlaw Conference Forum is EMCISnetlaw02alina
Draft Copy, not proof-read

Computer Threats in the Digital Age

Trust and Security in an Electronic Age
Protection of the Electronic Infrastructure

by
Nick Lockett,
Stanbrook.com technology Law Group

This paper is written at an introductory level and technical aspects of threats has deliberately been left out in many cases.
The views addressed in this paper are the personal opinions of the author

Introduction

In less than one generation, the information society revolution has introduced the computer into virtually every critical dimension of our daily lives and the economy. Even turning on the lights in our homes is dependent upon the internet for communication - as information is fed via the internet to the critical infrastructure of electricity generators and distributors and used to control power-load and power-demand information. In many cities, the traffic flow and public transport systems are now managed by computer systems.

In May 2002, a simple computer error in a new radar system brought air-traffic chaos in the UK. Later the same day, a computer error in Belgian air-traffic control disrupted matters further and the effects were experienced throughout the whole of Northern Europe. This highlighted the interdependencies of the airlines on computer infrastructures and the fact that the systems could not easily cope with two or more simultaneous failures, a concept not previously thought statistically liable.

The European Union recognises in its framework proposals about Attacks of Information Networks that it is possible to launch an attack from anywhere in the world, to anywhere in the world, at any time and that new unexpected forms of attacks could occur in the future. As the attacks against information systems constitute a threat to the achievement of a safer Information Society and an Area of Freedom, Security and Justice, it is appropriate that the response is made at European Union level and this will use both the European Arrest Warrant and the new proposals to expand the jurisdiction to extradite for cyber-attacks.

An attack against an “information system” is an attack against any electronic communication networks or systems they connect with including “standalone” personal computers, personal digital organisers, mobile telephones, intranets, extranets as well as networks, servers and other infrastructure of the Internet.

CRITICAL INFRASTRUCTURE

The new age carries within it a new peril. All computer-driven systems are vulnerable to intrusion and destruction and even where all possible steps have been taken to make intrusion virtually impossible, a loss of service through connectivity can be almost as critical, albeit that safety is not a factor. A concerted attack on the computers of any one of our key economic sectors or governmental agencies could now have catastrophic affects.

Hostile powers, terrorists and criminals can now use a potent weapon that is capable of doing enormous damage and yet is on sale in every highstreet and for which the information on how to use it is readily available online. . If we are to continue to enjoy the benefits of the Information Age, preserve our security, and safeguard our economic well-being, we must protect our critical computer-controlled systems from attack as well as protecting our citizens against the denial of use of the e-infrastructure, the theft of their information and the e-forgery of identity.

The question of Critical Infrastructure Protection (CIP) is not a post-September 11th measure. In the USA, the first US CIP Presidential Directive (No. 63) was issued as long ago as May 1998. This involved the analysis of vulnerabilities and regular updates as the understanding of the emerging threats evolves.

Critical infrastructures include the sectors of information and communications, energy, banking and finance, transportation, water supply, emergency services, and public health, as well as those authorities responsible for the continuity of national and local governments.

To ensure effective Information Society protection and security there will need to be a co-operation and openness between government and the private sector unlike any we have seen before.

Defence of our cyberspace will rely on new security standards, multi-layered defensive technologies, new research, and trained people. Of all these, the most urgently needed and the hardest to find are the computer science/information and communications technology (ICT) specialists who understand the security issues and the threats.

In April 2002, the European Union Proposal for a COUNCIL FRAMEWORK DECISION on attacks against information systems was published earlier this year and is annexed hereto.

Growth in Computer Crime

The volume of computer crime and security incidents is growing rapidly and is now about twice the level of 1999. The threat of external attack has now surpassed the threat of internal attack in a number of countries for the first time and the areas of greatest financial impact remain laptop theft, data or network sabotage, virus and Trojan infection, and computer-based fraud.

The majority of security administrators (about 75%) identify independent hackers as the most likely source of attacks on their network, followed next by disgruntled employees or contractors at 50%. Only 25% thought that foreign governments and foreign corporate competitors were likely sources of attack. Government agencies with national security classified material, companies which have developed or are developing profitable innovations or who are operating critical infrastructures are likely to be the targets of cyber espionage and/or sabotage.

The arrest of large groups of hackers suggests that hacking could increasingly be an organised crime phenomenon. There have recently been sophisticated, organised attacks against intellectual property as well as attempts to steal substantial funds from banking services.

Reporting incidents

Pessimism regarding the apprehension of attackers is the primary inhibitor to greater reporting. While more organisations as a percentage are experiencing attacks, fewer organisations are reporting that they don't know if they have been attacked or not. Computer attacks, being surreptitious in nature, means that detecting them can be difficult. Sophisticated hacking tools like root kits, loadable kernel modules and log scrubbers, which enable attackers to cover their tracks once they have gained privileged access are now available.

Cyber espionage and sabotage?

There are numerous examples of national security agencies deliberately or inadvertently tipping off their national manufacturers about the bids likely to be put into a tender by foreign companies. The reality is that if foreign governments and corporate competitors choose to direct such activity towards their adversaries or competitors – and many do, they will have at their disposal, more sophisticated computer attack skills and resources than your average script kiddie. Yet despite this, the number of organisations that encrypt their data when in stored form and use secure systems to check that the computer doesn't retain a temporary unencrypted file is disappointingly low.

Only if organisations fully understand and recognise the nature of the threat they face, they will be in a position to more effectively manage it. A sufficiently skilled hacker can steal information and the attack may never be detected or if suspected, is completely devoid of forensic trails, but if the information is securely encrypted then it is useless to the hacker even if stolen. Current estimates are that over 40% of unauthorised network accesses are motivated by the desire to obtain sensitive or proprietary information for personal, political or commercial gain.

Echelon

The role and impact of Echelon is fully covered in the EU Report and will not be covered in this paper

Criminal Investigations
To carry out effective computer crime investigation requires a Hi-Tech Computer Crime Investigation Unit which should be a career post to avoid police officers being moved between regions and between specialities. Regional Hi-tech Crime mobile cyber-busting units should also be available for major incident responses and trained and equipped for sound computer evidential seizure and to response to incidents such as DDoS (Distributed Denial of Service - or DOS)

Assisting CyberCrime prosecution
The legislature must consider whether, in the same way that some jurisdictions protect rape victim anonymity, the reporting restrictions on computer crime should not name the victim or the method of the attack (or that evidence is not given in public).

The lack of confidence in law enforcement's ability to catch and successfully prosecute the perpetrators and lack of realistic sentences must also be addressed. If a person enters a bank with a shotgun, they risk and often get serious prison sentences, but attempting to steal potentially significantly higher sums electronically in a manner that could cause the collapse of the bank due to lack of confidence will be perceived as a less serious offence. The legislature must realise that this is going to be a future route of funding terrorism and organised crime and sentence anyone guilty of financial online attack accordingly.

The legislature must also address the genuine difficulties faced by law enforcement agencies in identifying and tracking perpetrators of computer crime, particularly when the forensic trail crosses international borders and jurisdictions and when various parties – either the victims or others used to facilitate these crimes – have inadequate logging or user identification and authentication in place. In some cases, the European Arrest Warrant and new provisions to require CSPs to put into place audit trailing facilities go someway towards assisting this but there is still a long way to go.

Monitoring and Audit Abilities
CSPs (Communications Service Providers) are required in many Member States to maintain audit trails for a short period and to put into place complex monitoring facilities

In the attack on greengrocers.com.au the audit trail received from the telecommunications company showed a remote connection immediately prior to the two incidents originated from an IP address belonging to a cable modem customer, who was identified as a former computer network engineer who had resigned from company a few days previously. The engineer simply deleted critical router files, rebooted the router and caused loss of the Internet connection. In the second phase the engineer used the company's pcAnywhere application to remotely access a server and delete critical operating system files causing the server to fail, access was possible as his passwords and access codes hadn't been changed immediately on his departure. Although the damage to the company was serious and sentences carried a maximum sentence of 10 years imprisonment per count, the engineer received an 18 month suspended sentence, hardly a deterrent.

Critical Infrastructures

We know of foreign governments creating offensive attack capabilities against critical infrastructure networks. In the opening days of the Kosovo crisis, certain major organisations in London including banks and insurance entities came under sustained military-grade cyber attacks.

The infrastructures at issue are largely privately owned and they have a substantial economic stake in protecting that investments and ensuring the continued operation of their systems. In general, those who own and operate these systems are in the best position to understand and prioritize this range of threats and what is necessary to mitigate them; however a critical step to establishing a sound and acceptable infrastructure protection program is for the government to explain what it expects to bring to the issue that is not already being addressed by private sector's existing security programs and what funding may be available. In particular private sector operators of critical infrastructures are being expected to develop defences without fully understanding what they were defending against and in this respect, Government, the military and the intelligence services must play a role. In some cases the sharing of foreign counterintelligence with industry will create unique challenges of protecting sources and secrecy.

In the same way that industry technical standards bodies spent years developing digital switching equipment to accommodate law enforcement needs for continued ability to perform court ordered interception and additional capabilities, so this requirement is being imposed on CSPs in Europe.

There is no lack of Information Infrastructure Security Standards, but only very recently has Europe realised the need to create a pan-European Critical Infrastructure set of standards and evaluating standards or the methodology of improving standards leaves much to be desired. Another element of Government and European contribution in the creation of infrastructure protection is the provision of vulnerability assessments and warnings of pending online attacks which will need to draw on the skills of information warfare specialists and security intelligence reports although it is unclear what level of assistance Governments in Europe can safely provide without compromising secrecy and in the new era of anti-terrorism, the question of compromising secrecy and the balancing of Critical Infrastructure protection must be addressed.

Other issues for businesses running Critical Infrastructures are the degree of business secrets they are prepared to provide and the question of confidentiality. In some cases such as provision to Intelligence Services, these concerns will not arise but other disclosures, such as to standards bodies and government departments may raise particular secrecy concerns. A number of private initiatives involving financial services organisations aimed at the sharing of information on online threats and attacks, incidents and vulnerabilities among banks and other financial institutions exist but have deliberately not involved or forwarding information to the national government for fear of leakage. Governments need to consider whether the role of the Intelligence Services

in receiving national information and anonymising it for use by other organisations should be expanded and the legal mandates involved in such steps.

The reality is that critical infrastructure protection plans are largely based on indirect, market-based necessity incentives, rather than legislative requirements although Governments carry out increasing roles in encouraging the development of best practices and appropriate information security standards, including adherence to new information security standards as part of licensing conditions and via Government encouragement through insurers coverage standards.

In some areas, the standards may not be sufficient as in government and private sector telecommunications networks where there is a critical need for "early warning and response capability" and monitoring of such items as near real-time monitoring of the telecommunications infrastructure, anomaly and attack profile recognition and the capability to trace, reroute, and isolate electronic signals that are determined to be associated with an attack. In many cases these have moved into non-critical multi-national organisations as essential infrastructure protection requirements.

Issues arising from Infrastructure Protection
It has become increasingly apparent that current law has failed to keep pace with technological developments and therefore that current "data protection" laws and "interception practice" have been out of date with modern technology and the needs of modern law enforcement. Some European Countries have amended their laws to bring these up to date although whether this will result in an appropriate balance, infringement of private rights or a lack of abilities on law enforcement agents remains to be seen.

The Governments must decide whether the privilege of operating a critical infrastructure means that there should be compulsion in information sharing and although the voluntary nature of industry participation is preferable, the methodology of any compulsion must be carefully considered. It must also consider how identification of critical assets will be achieved, how preliminary vulnerability assessments will be made and how mandated security processes (if any) are to be put into place. Given the strong market-driven incentive to encourage good security practices, Governments will need to consider how any mandatory operations are to be funded from corporate and government budgets and how Computer Emergency Response Teams will be operated, secured ad funded. They will also have to consider how interdependencies might arise when an infrastructure is attacked and what the appropriate commercial and market-orientated solutions are.

Governments in Europe will also have to consider whether Critical Infrastructure employees can be subject to employment vetting that would not be allowed for the general population

ICANN
ICANN was originally set up to operate the rules for the global internet names – or gTLDs. It was not envisaged that ICANN would do anything other than operate as a lightweight consensus-forming structure providing good practice guidelines and

managing the roll-out of new domains in the global internet space (such as .info, .biz etc). Unfortunately somewhere along the formation discussions and against the advice and wishes of many influential internet gurus, it persuaded the US Government to give it the operational IANA root function which maintains a handful of critical functions such as the database of ccTLD managers and critical servers. At present it is the only current option.

The original ICANN concept was a consensus bottom-up policy formation body which would gradually over time become less active as the internet infrastructure problems were solved. It would have recently increased operations as security concerns arose but the aim was an increasingly less operationally interfering structure. Instead we have an organisation which has just removed the at-large internet community consultancy ability and which has been taken over by commercial interest.

Much more worrying for the European Network Security is the increasing control of the organisation by American interests and the refusal to take into account the needs of the non-US ccTLDs. To fully extrapolate the issues raised would take a thesis but there are a number of key points:

a) ICANN has become the Single Point of Failure that the Internet was designed to avoid. There is a complete lack of formal relationship regarding root-server operations which are the core systems upon which the entire internet is dependent. There are still run on a pro-bono basis by volunteers despite the funding of ICANN to the tune of millions of dollars per year which, in my opinion and the opinion of others, ICANN appears to squander on an increasingly inefficient and inept administrative bureaucracy.

b) The excessive influence by domestic interests in the US and US Government over domain name and DNS means that Policy authority over the legacy root system is asserted by, and de facto controlled by the United States Department of Commerce. Some experts say that this has the potential of being seriously detrimental to EU trade interests – for example the Department of Commerce has the final say over whether and how a .eu domain will be run as it has the ultimate policy control.

c) Recently ICANN has shown signs of being increasingly desperate to obtain additional funding and power and has turned its eyes on the national or “country code” (ccTLD) domain registries (such as .uk, .fr, .si). It is an organisation grown out of control and now appears to be trying to sign ccTLDs up to the existing US-centric one-size fits all structure of ICANN – a role which it has demonstrated itself to be incapable of fulfilling. Having spectacularly failed to achieve anything like a consensus amongst ccTLDs that it even has a role to play outside the gTLD area, it is now picking off the ccTLDs one at a time by what appears to be a misuse of IANA function. The IANA function is simply a lightweight database function which includes the details of the ccTLD registry managers and their servers. In its fight to control the ccTLDs and to force them into its rigid and costly structure it is now refusing changes to IANA database and using the threat of "No amendment without ICANN contract" as bargaining chip to enhance its commercial aspirations. This creates an unacceptable destabilisation and security risk and in my view

evidences ICANN as unfit to carry out the IANA role. The ICANN contract, in the opinion of many including myself, is entirely unsuited for ccTLDs and will stifle growth.

In this IANA role, ICANN is also insisting, under the spurious argument of security, on copies of local ccTLD domain-owner databases being transferred to the US despite the European data protection issues. There is simply no technical reason why escrow of the databases needs to be anywhere other than in the national country of the ccTLD. A signed-up ccTLD means more money for ICANN.

An organisation as critical as ICANN should be an international treaty body, not a body with commercial aspirations which significantly considers US interests to be primary. Despite being an exponent of public relations and self-serving spin, its ICANN's CEO has recently described it as having failed in its original mission and litigation has broken out even between the board members over allegations of secret documents and breaches of US (California) law. It is already showing signs of a lack of internal confidence as evidenced by a high turnover of senior staff and any organisation in that degree of crisis is not an organisation that is left with the necessary credibility to be in charge of the core of the internet - a single point of failure by its own choosing.

CERTS

Organisations also need to be encouraged to have Computer Emergency Response Teams ready for a security incident and this will include not only IT specialists but also legal counsel familiar with the issues and already prepared to take the necessary actions within the legal framework and to preserve forensically admissible evidence. The legal counsel must also be able to think outside the usual parameters so that they can advise against or accommodate the wish not to pursue legal options. One other role that the independent legal counsel can also do is to act as an anonymous source of information to the hi-tech police crime units so that the police are aware of the issues arising. The police must in turn respect the concerns about negative publicity, creation of competitor advantage by reporting and the risk of turning organisations in similar positions into targets.

Heightened Risks

The increased connectivity and use of Internet services provides increased opportunity for attacks and coupled with increasing complexity and therefore vulnerability of computer software, we are only just entering the world of the electronic crime. When you add increasing use of high speed Internet access for home users such as ADSL there is increased vulnerability to the executive working from home. The pace of technological change means that increasingly powerful machines are now available to hackers and users are too slow to adopt good computer security practices. Even where they do adopt computer security this might be fundamentally flawed (as the recent felt-pen defeat of Sony's CD protection system and the Vaseline defeat of biometric fingerprint systems have shown).

- lost business opportunities,
- erosion of consumer confidence
- cost of misuse or degradation of network performance

- cost of investigation and recovery

In-House Insecurity and Insecure Private Keys

We have data protection securing data whilst at the same time we are becoming more reliant on digital signatures as authentication but unfortunately there is also a new breed of problems about to emerge – the trusted insecure digital signature. Europe has gone down the route of digital signatures – probably the only route available to it at present – but has failed to achieve a safe route because it has given into commercial pressure and made life as a digital signature provider too easy.

Digital Signatures are only as secure as the process by which they are issued, stored, used and maintained. It is assumed that if a message is signed with my digital signature then only I could have signed it. The failure comes about because the legislation failed to require the digital signature provider to provide the recipient of the key with a mandatory safe way to hold the private key. As society begins to trust digital signatures more and more, compromised digital signatures will occur where the legitimate holder has no idea that their private key has been compromised because they have failed to properly secure their home or personal computer.

Digital Certificates have one other massive flaw, that they assume that provider of the certification did actually carry out a correct identification of the person to whom the key was issued. Relying on the certification agency is a massive leap of faith and the terms and conditions of most certification agencies are so restrictive that the possibility of action against the certification agency will only arise in the rarest of circumstances. Entrust's Certification Practice Statement states that Entrust does not "*make any representation or provide any warranties with respect to the techniques used….. reliability of any cryptographic process …..software ….. repudiation of an Entrust web certificate .. or any transaction facilitated through the certificate"* whilst Verisign similarly disclaims *authenticity, reliability, completeness, currentness, merchantability or fitness of any information in the certificate [or otherwise in any way associated with it]*

Many Trojan programs are designed to be capable of looking for user's signatures in signing into other networks or on-line banking facilities. Reports have recently been circulated of a new viral-worm designed by the FBI to secretly record private keys from encryption systems so that the FBI can subsequently read even encrypted messages. If this is true the risk is that US anti-virus developers will be persuaded not to detect such activity as a virus and it is only a matter of time before the hackers exploit the process to develop undetectable sniffer programs based on the same viral-worm fingerprint as law enforcement authorities.

By far the easiest method of getting use of someone else's digital signature is to get access to their computer. In some cases, stealing a computer gains access to the key, insecurely stored as well as the only copy of the revocation procedure held by the true owner of that key. Although the law is clear about where liability arises in the event of fraudulent use of the key, the law is entirely unclear about the user's liability for storing the key in an insecure manner. In theory, I could be entirely absolved under legislation

and caselaw from any liability arising from the use of my stolen key but then found to have stored the key in such an insecure manner that some degree of liability arises again.

Identity Theft

From the compromise of the private part of the Digital Signature key comes something that is already an unspoken epidemic in Europe – electronic identity theft.

In its minor form, this is junk mailing or spamming where the apparent sender knows nothing about a mass mailing. It has been going on for years and yet the legislation has failed to comprehensively make the use of false electronic identities unlawful – hardly surprising given the length of time it has taken Europe to decide on whether the relatively simple issue of opt-in or opt-out should take. The transmission of a false electronic identity and the aiding and abetting of this must be made unlawful. There are a handful of entirely disreputable ISPs who willingly provide facilities to these spam agents because of the lucrative ISP supply contracts and they should be subject to a requirement to prohibit transmissions when placed under notice and to refuse to provide facilities to the organisation who regularly spam the internet. As the incentive to comply, they should be open to unlimited liability for the costs of the recipients in processing the mail and a European-wide, and preferably a US-European accord under communications law should allow for easy enforcement of claims and licence suspensions.

More worrying is the entire theft of a person electronically. This typically starts with the theft of a briefcase or handbag or (rarely) a computer. With minimal paperwork such as a Credit Card it is possible to start setting up utility bills. The time delay inevitably means a delay before identification of that fraud arises. With the utility bills and credit card, further apparently valid identification documents are able to be applied for. Although credit cards and utility bills are accepted as one of the primary sources of identification, their validity is only very rarely checked.

The advent of the online world has meant that people are storing on many internet sites, their security details and in some cases they use the same password as used for their online banking systems and work computers. A maiden name or mother's maiden name or date of birth are matters of public record but even if they were not, once given online they cease to be useful as any future identify verification. In many cases following a theft, a phone call is received from the fraudster pretending to be the bank and asking for the victims details for security verification, cleverly feeding the information that is public or compromised to get other unknown information. Once that information is known, a full electronic identity can be set up or manipulated. From that point onwards, almost anything goes. Simple precautions such as giving online sites different information (except critical sites such as online banks) can help to stop identity theft. For example a mother's maiden name of Copper becomes Iron except for your online bank and a date of birth of 10th August 1960 becomes 8th October 1960 (month and day transposed) .

People are finding that they have car and house loans through online checks using chains of documents establishing the forged identity and in the electronic world this is becoming easier and easier. Governments will soon need to consider whether to criminalise the use

of any form of false electronic identity although this also creates a mountain of legal issues.

Attitude to Security & Protection

Attitude is the most significant barrier to improved security although failure to understand firewall and basic security configuration although failure to properly manage software upgrades and bug patches in complex IT infrastructures is a close second. A worrying number of organisations have failed to realise that their key business asset is now their IT infrastructure and that simply ensuring back-ups are taken is not adequate. Take the chemical company which recently interviewed a candidate who was able to tell them about their new top-secret product – information gained by 3rd parties from listening to the wireless network and selling the information to the nearest competitor.

Typically the figures for protection are:

- password protection (100%),
- anti-virus software (99%).
- physical security (locked doors etc) (91%),
- access controls (95%),
- firewalls (95%), (but these may be insecure out of box configurations)
- encrypted login/sessions 50%
- encrypted files 45%
- digital IDs 45%
- smart cards 35%
- biometrics 5%,

Most companies now have basic computer security technologies but have failed to use stronger authentication and encryption technologies or to have implemented an overall security policy framework which makes provision for monitoring and maintenance of their technology and information systems.

The rapidly changing nature of the attacks and vulnerabilities and the increasingly sophisticated and powerful attack tools provide low-skilled attackers with an easy to use interface into networks. Network and system administrators have the additional burden of getting network defence right all the time whereas an attacker needs to find only one point of vulnerability to do damage and the cost to European Network administrators of the availability of scripts etc runs into many millions, if not billions, of Euros per year.

Firewalls

Firewalls are rarely configured for maximum security as this makes them less easy to install. Unfortunately this means that the most “out of the box” firewalls are easily defeated. Government initiatives to encourage manufacturers to set default firewall settings at maximum security would mean that less avoidable intrusions would occur.

The failure to note Vendor advisories and apply the recommended fixes, leave organisations vulnerable to attack. Attackers succeed in exploiting vulnerabilities not yet in the public domain and for which vendors have no available fix and have therefore not

yet announced the vulnerability. Sound computer security practices and well developed incident recovery plans minimise risk

Firewalls continue to be relied upon as perform a more fundamental role in network security and far too few companies use intrusion detection systems (IDS) as an adjunct to network security. Less than 50% of European major multinationals have implemented IDS and at the SME[1] level they are rare. The perception remains at board level that a firewall is a cure all defence but because firewall permit valid web traffic, they cannot protect against web-based attacks and the technology only aids risk management and mitigation. Jurisprudence is beginning to emerge suggesting that a failure to appoint an IT competent security director at board level may be negligence by the board members and it is only as directors become personally liable that responsible IT security management will be achieved.

Wilful and stupidity failures

In another recent case, an organisation discovered that its valuable confidential and strategic information had been leaked to a competitor although initially a contractor was suspected. A thorough investigation was conducted to determine the cause and source of the leak and an employee of the service organisation was found to have used the confidential document as a style template but inadvertently failed to save the changes to the document which would normally have removed the sensitive content. The employee e-mailed the unsaved template to another of its clients and an employee at the recipient organisation realised the significance of the document and promptly sold it to the organisation's competitor. Unfortunately for the seller, the recipient organisation had entered into a confidentiality agreement covering confidential information acquired directly and indirectly and was liable for the whole of the loss.

Unauthorised Additions

Despite latest anti-virus signatures, software patches and an awareness of the nature and impact of ongoing changes to their network architecture and environment by a good systems administrator, the simple installation of an unauthorised modem in order to gain faster access to the Internet could bypass the firewall, IDS and virus checkers. The use of an unauthorised wireless link, often one advertised as network neutral and simply plug and play, may not even be notified to the system administrator but may make the entire network vulnerable. It only takes one small transgression, such as a trial copy of software, to obtain back-door Trojan software which gives undetected network access to a hacker.

Laptop Losses

Laptop theft ranks as the most costly computer crime and in the UK it was recently confirmed that the largest government department losing laptops was the Ministry of Defence with the Inland Revenue not far behind. It does not necessarily follow that laptop theft poses the single greatest threat to an organisation's computer and network security as secure systems can be useless if stolen. Sensitive data on my portable is stored

[1] Small and Medium Enterprise

in an encrypted area of the computer and an easily removable PCMCIA memory card needs to be used to access that area.

Laptop theft is however potentially the conduit for theft of confidential or proprietary information or the means by which remote privileged access to a network is achieved. In many cases, the incompetence of users means that a laptop is set to automatically access a corporate network so if stolen it provides a short window of opportunity during which Trojans and other malicious software can be introduced into the corporate network.

On-line merchants failing to secure

Use of bogus and/or unauthorised credit card numbers on e-commerce sites is increasing exponentially due to the failures of on-line merchants to employ personnel with adequate experience in Internet security. They fail to take even the basic steps to protect their own interests and the interests of legitimate customers who provide their personal and credit card details resulting in unauthorised debits and legitimate users having their cards blocked because of unusual transactions which might be internet misuse. In many cases, the guilty companies were of significant size and had been trading for a number of years in the retail markets. British Gas was but one of the major British companies, like companies throughout Europe which had failed to secure its online access properly. Another French company had no validation processes in place for either the purchaser details or credit card details and therefore unsurprisingly had failed to record vital transactional information (inadequate customer identification and validation and transaction logging) that would enable an offender to be traced.

Card attacks result in increased opportunities for payment fraud and force the banking industry to cancel and re-issue thousands of cards at a huge cost and although e-commerce merchants offering. A further consequence is the intangible damage to the merchant's reputation and to consumer confidence in e-commerce. Preventive measures, such as minimum security requirements for online merchants accepting payment cards, are being discussed under the EU Action Plan to prevent fraud and counterfeiting of non-cash payments but the market solution will be banks suing online merchants for costs involved with re-issue of cards

In a recent case, a police Computer Crime Unit arrested certain suspect on suspicion of obtaining and re-selling stolen computers only to discover a hacking factory. This group had penetrated 8 banks in the city concerned without the banks being aware that they were being hacked or that funds were missing from their accounts. The team included an ex-bank manager forced into early and unwanted retirement who knew where and how to hide the transfers. The team had also managed to infiltrate a public Internet café and had their own computers not been found, tracing would have been impossible from the café. Unfortunately criminals of this technical competence are rarely caught and it is difficult to know what the true levels of undetectable hacking skills are in use. What is certain , there will be an increase in the types of crimes that exploit these security weaknesses. To prevent future occurrences, on-line banking sites may need to make their client identification and authentication processes more secure, for instance, by the use of

challenge-response or one-time passwords or physical security tokens which can be plugged into computers.

Hackers & their Motivation

These are children or adults, ranging from the otherwise lawful to professional thieves, some are members of organized crime groups, terrorists, potentially hostile military operatives or members of foreign or domestic intelligence services. Even domestic intelligence services hack. Every day, thousands of unauthorized attempts are made to intrude into the computer systems that control key government and industry networks: defence facilities, power grids, banks, government agencies, telephone systems, and transportation systems. Some of these attempts fail. Some succeed. Some succeed when there is no excuse for them to succeed.

Typically hackers are trying to

a) obtain "systems administrator status,"
b) download passwords,
c) implant "sniffers" to copy transactions,
d) or insert trap doors to permit an easy return
e) obtain financial gain,
f) cause malicious damage (eg, web site defacements)
g) programme attacks (DDoS attacks, release of viruses and worms)
h) theft of network resources (eg, bandwidth usage) for personal use.

Some attacks use Kiddie Scripts – the equivalent of car thief "joy riders," and doing it just as a thrill. Others are committed for industrial espionage, theft, revenge-seeking vandalism, or extortion. Some may be committed for intelligence collection, reconnaissance, or creation of a future attack capability. Some companies have even been pre-vetted so that attacks can be co-ordinated at a later date when the company is particularly vulnerable and to cause maximum share-price loss. What has emerged in the last several years is an increase in the seriousness of the threat.

Availability of hacker tools

The distribution of powerful and easy to use attack tools online or via the public domain is not an offence in most European countries. This is because legislators are worried that legitimate security analysis software would become unavailable to system administrators. In reality, most companies would readily accept legislation requiring checks similar to an online money laundering check – to ensure only legitimate customers get access. Companies cannot take this role because they cannot guarantee their competitors will take the same responsible actions. Again, the role of CSP liability once on notice would prevent further distribution.

The European "attacks of information systems" proposals cover the notion of "hacking" where a person hacks into gaining unauthorised access into a computer or network of computers, usually by exploiting inside information, or by a brute force attack or password interception. The provisions are usefully drafted because they cover unauthorised access where a password system is in place but where it is ineffective

(usually due to a default set-up) as well as access to services protected by conditional access without payment. The use of access to an information system is also clearly designed to cover the sniffing of wireless networks (war-driving) without presence in the system or intrusion onto the network.

Trusted Insiders

For the first time in 2001, Internal attacks were less common than external attacks (by a factor of about 20-30%) which contradicts the popular belief that most attacks originate from the inside and that companies should focus more on their employees. The risk has now shifted. That is not to say that the threat from insiders should not be underestimated – for well-protected systems the greatest harm will still come from insiders.

Types of Attack

Insider abuse of internal computer resources
Insider abuse of internet access or e-mail
Unauthorised access to information by insider
System penetration by outsider
Laptop theft
Virus / Worm / Trojan infection
Telecom eavesdropping
Wiretapping
Degradation of network performance associated with heavy scanning
Denial of Service (DoS or DDoS) attack
Sabotage of data or networks
Telecommunications fraud
Financial fraud
Unauthorised privileged access
Theft / breach of proprietary or confidential information

DDOS

There has been a massive growth in incidents of computer infrastructure abuse such as Distributed Denial of Service DDOS Attacks and offences which begin with external port scanning. In the modern environment, DDOS should not occur. DDOS occurs because computer administrators fail to set sufficient security on their systems to prevent them being hi-jacked. Yet legislation in many European Countries, many years after DDOS attacks began still presents almost insurmountable hurdles to prosecution because they have not been updated. Straining some of the old laws of common law jurisdiction, such as Rylands v Fletcher, a civil liability can be established but there is a simple two-step process to preventing such attacks.

Step 1: Education about liability provided by specific codes relating to failing to adequately secure large computer systems.

Step 2: Enforcement of liability

In many cases, the hijacked computers are educational establishments who have no real incentive to prevent the attacks but as soon as the case of liability arose under Codes, the University administrators would ensure adequate funding of systems.

The European "attacks of information systems" proposals covers many of the disruptions of information systems, including malicious attacks, distributed "denial of service" attacks (DDoS)[2] as well as malicious software, virus distribution, logic bombs, Trojan Horses and worms.

War Driving

External port scanning, without legitimate excuse, should be also an offence. The trend towards wireless networks has a short-term and very worrying security implication, namely the risk that wireless networks can be "sniffed" or listened to by anyone in the vicinity. Certain software tools on the internet can break network access security systems within a few minutes on the average corporate network. This allows hackers to enter the system and from that point they are committing the classic unauthorised access offences; however the hacking laws are written to look at unauthorised entry into a computer system and not the unauthorised overhearing of a computer system.

Just overhearing a computer speaking to its network by sitting in a car outside a building is not gaining access to the network except in the most strained of legal interpretations, to argue otherwise means that a telephone message is intercepted when a telephone call is overheard through an open window. Clearly both are currently lawful. Here the legislators have a role to play because the listening for a computer nearby is a much more active step than the average overheard telephone conversation and many countries could amend their law to prevent this abuse. A radio station recently reported that by driving around the area of the European Commission in Brussels, it was able to listen into over 140 networks – NOT, I hasten to add, the Commission networks (nor the Stanbrook network which is not wireless) but the internal network chatter of the nearby companies lobbying the Commission and advising on mergers and their competition aspects. This information in the hands of terrorists would highlight very price sensitive information and as organised crime, that is the area around which I would park my little white van to gain the information I need for funding my other activities.

Worm-induced network degrading

During the latter part of 2001, a spate of new-style worms increased the problem. They emerged with a higher level of scanning which means they were increasingly skilled at looking for new hosts to infect. As they do so, they significantly degrade network performance. In just 9% of the case sampled in Australia, the degradation reported was of sufficient severity that 9% of organisation experienced financial losses in the vicinity of over $160,000 in lost productivity and manpower.

---

[2] DDos attacks occur where machines are flooded with repeated requests for access faster than they can process them. This is done in an attempt to .
Denial of service attacks attempt to overload web servers or Internet Service Providers (ISPs) with automatically generated messages. Other types of attacks can include disrupting servers operating the domain name system (DNS) and attacks directed at "routers". Attacks aimed at disrupting systems have been damaging for certain high profile web-sites like portals and ccTLD registries.

Web Site Incidents
About half the attacks were DDoS attacks, followed closely by web site vandalism. Although worrying, this is at least visible. Other potentially more serious forms of attack involve financial fraud and gaining unauthorised privileged access, theft of transaction information and theft of intellectual property.

Financial losses from web attacks are small although as organisations build in greater functionality and more online services, they become more dependent on web-based revenue and the potential for more damaging attacks will increase. We have already seen a number of online merchants collapse following web attacks.

Computer security challenges
Despite a relatively high uptake of basic security technologies (passwords, firewalls, anti-virus software), serious computer network attacks continue and will always continue to occur. How the security of the network and user inferfacing with the network is managed and the extent of good computer security practices will also have a bearing on how well organisations minimise their risks. The real step forwards will occur when there is a full understanding of the need for staff training about security as well as the need for an examination of the process-related network security activities (such as not installing insecure default programmes). Configuration management - the process of managing changes to the network architecture and systems – needs to be managed securely

Board-level understanding about proper investment in Infrastructure security to counter new and emerging threats and vulnerabilities is needed and must be backed by Government initiatives. Users must understand, and again only Government is in the position to do this education, that such activities as the installation of a new Internet connection, the need for remote access, or the enabling of Java, ActiveX or downloading other executables and software have security implications and that in a broadband world updating of anti-virus and use of IDS is essential

For organisations whose networks perform business critical services, the installation of patches generally occurs first in a test environment which allows network administrators to identify any potential software conflicts or network failures caused by the patch. This is generally accepted as good for security and business continuity because loss of the Network Infrastructure is a loss whether arising from an attack or from incompatible software; however business decision makers must be made aware that one limitation of first applying patches to a test environment is that it increases the period during which weaknesses can be exploited.

IT managers and their staff have to work in an environment in which their organisations are becoming increasingly dependent on the network infrastructure to support critical business services and, therefore, must work under the pressure of higher expectations of uninterrupted availability and increased functionality, but effectively managing computer and network security is a complex and challenging task, even if adequately equipped, experienced and resourced.

Thank you to the organisers for the opportunity to provide this talk and thank you for reading the above. If you have questions please use e-mail or the discussion group online at www.netlaw.co.uk (follow the Slovenia Conference links).

Nick Lockett
Stanbrook.com Technology Law Group
www.netlaw.co.uk
nick@lawyers.co.uk
T: +44 70920 70120
F: +44 870 133 9104