ISSN. 1363-6650

OCTOBER 1997
Issue 10

International Journal of FORENSIC COMPUTING™

Contents

International Journal of Forensic Computing

Third Floor, Colonnade House,
High Street, Worthing,
West Sussex, UK
BN11 1NZ

Tel: +44 (0) 1903 209226
Fax: +44 (0) 1903 233545
e-mail:ijfc@pavilion.co.uk
http://www.forensic-computing.com

Comment

The science of computer forensics is in its infancy. Those working at the sharp end of the business - the police forces, investigators, lawyers and analysts - know that it's pretty much an undiscovered country that is only just beginning to be explored.

Computers, while a fundamental part of modern life, have only been around in any number or degree of usefulness for the past 25 years or so. In the scale of human endeavour that is minute and this is reflected in many people's attitude of antipathy towards anything silicon.

Many simply can't grasp the implications of what computers can and cannot do, while others are so scared that they won't understand how to use the technology, they ignore it all together.

This notion that all things computerised are a black art best left to the scientists and technicians is symptomatic of this and is endemic in society.

But this prejudicial notion is not only a waste of opportunity, but carries with it extreme danger if the police, law enforcement agencies, government bodies and legal personnel take a similar view.

After all, those joining these professions are part of the same society and it is therefore unsurprising to find a high number of them shy away from learning about the power of computers for both use and abuse.

Computers are everywhere in the Western world, yet most police forces in individual countries have tiny computer crime investigation departments, often with just a handful of staff, little in the way of resources or equipment, and woefully inadequate funding.

With this level of commitment they can only be skimming the surface of the huge pool of computer crime, which by its very nature can be almost impossible to spot. A murder leaves the tangible evidence of a dead body and bloodied knife, where as a hacker can bring a company to its knees using just a few clicks on his mouse, quite feasibly leaving little or no clues.

True, computer crime does not carry the same emotion laden values as violent crime or burglary, but its effects can be just as hard-hitting and permanent.

The fact is that until computer crime is thoroughly investigated, the true levels it has reached will not be known. There is a massive iceberg out there and we have only just begun to see the tip of it.

There is hope though, and with luck we will soon be entering a new phase in how computer crime and evidence is tackled.

The issue is beginning to make news headlines across the world as people begin to see that it isn't just about nerds trying to hack into the Pentagon.

Multi-million pound fraud, hardcore child pornography, viruses that can wipe data instantly are all accomplished with a computer and a little know-how.

Within five years the topic and its importance will have grown beyond all expectation and it's vitally important that everyone involved is prepared now.

This means assembling the laws, skills, resources and funding to address computer crime properly. By the time it reaches epidemic proportions it will be too late.

The Journal would be happy to receive any submitted articles, papers, case studies, technical tips or letters.

Articles are published on the understanding that publication is not taken to imply endorsement of the views therein by the Publisher or Editorial Team or members of the Advisory Board of the Journal. Courses of action described in the Journal in relation to one set of circumstances will not necessarily be appropriate for a different set of circumstances.

Accordingly, readers should take their own independent specialist advice before proceeding on any project or course of action and any failure to do so is at their own risk. No responsibility is assumed by the Publisher or Editorial Team or members of the Advisory Board for any loss or damage to persons or property as a matter of contract, negligence (save in respect of liability for death or personal injury arising out of any negligence) or otherwise, or from any use or operation of any methods, products, instructions or ideas contained in the material herein. Whilst all reasonable care is taken, neither the Publisher, nor the Editorial Team, nor members of the Advisory Board can be held legally responsible for any errors in articles or listings. Upon submission of an article, the author will be requested to transfer copyright of the article to the Publisher.

News

et fraudster jailed

The owner of an Internet newsletter in the S who pleaded guilty to fraud was sentenced a year in prison and fined $20,000.

Theodore Melcher Jr, owner and president SGA Goldstar Research Inc, admitted to nspiring to violate federal securities and tax ws by engaging in fraud through buying and lling stocks.

Prosecutors said that Melcher received ares of Systems of Excellence Inc, a maker video teleconferencing equipment, in xchange for publishing favourable reports out it, some of which were false.

US Attorney Helen Fahey said that lelcher, 51, from Brentwood, Tennessee, btained $515,800 in profits from the fraud d that most of the cash came through an ffshore company to avoid paying income tax.

She said that the case "should be a clear ignal to those who use the remarkable echnology of the Internet to snare vulnerable itizens in a worldwide web of deception."

Carles Huttoe, former Systems of xcellence chairman and chief executive fficer, last November admitted to breaking ecurities laws and engaging in money undering and received a 46-month prison entence in January.

White House pagers hacked

A computer hacker in the US claims he aptured private messages about President linton by using eavesdropping equipment.

Some of the messages included details of he president's whereabouts as well as nstructions, love notes and even basketball cores for agents and White House officials.

An anonymous young man handed a disk ontaining the information to Pamela Finkel, New York-based computer consultant. She ublished the messages on her own website because she said she wanted to show how easy it was to intercept private communications.

Finkel said: "I don't know if I'm going to win converts in Congress, but if I make them stop to think, this would be worth it. The information is more embarrassing than dangerous."

She added that all that was needed to get pager messages was a high-end radio scanner, a personal computer and hacking software easily found on the Internet.

A White House spokesman said: "We are aware that somebody has monitored paging traffic. Our paging system is not secure, so we'd know not to send unsecured messages."

Pamela Finkel's web page is at http:www.inch.com/esoteric/pam-suggestion/formal.html

Bogus identities using DTP

Thieves are using the latest technology to create phoney documents as part of fraud scams costing billions of dollars a year, a US Senate panel heard.

The Senate Banking subcommittee on financial services and technology was told that false identities could be created using easily available desktop publishing systems to get credit cards and to steal credit ratings.

Victims of the thefts have seen their credit histories ruined by thieves buying cars in their names or snatching pre-approved credit card application forms from mail boxes and changing the details.

The subcommittee heard that some offenders even sift through rubbish bins looking for old bills and documents with credit card numbers, social security details and bank account information.

Chairman of the subcommittee Robert Bennett said that cheque fraud alone cost an estimated $10 billion a year.

He said: "This is a growing problem and one that threatens to increase in the future because it is so easy to commit, difficult to track and perpetrators are less likely to spend time in jail."

One victim told the panel how her credit card history was ruined after her financial identify was stolen by an imposter who ran up a $28,781 bill on her accounts.

School psychologist Diana Christiansen said she had been in contact with credit card companies, retailers, state motor vehicle departments and law enforcement authorities and that the problem had caused "total frustration and anger".

Charles Owens, FBI financial crime chief, said: "Law enforcement is still confronting an increasing number of serious criminal referrals involving complex crime problems, many the outcome of emerging technologies."

The FBI has been involved in a group made up of federal agencies which hopes to combat the fraud dangers. Owens said: "A goal of the group is to ensure that adequate fraud prevention measures are implemented to assist in the detection, investigation and prosecution of individuals attempting to fraud the cyberbanking system."

Dana Brown, deputy agent in charge of the Secret Service's financial crimes division, said that the Internet "has vulnerabilities which can allow confidential business information and sensitive personal information to be compromised."

And Dennis Brosan, security director of VISA USA Inc, told the subcommittee that credit card fraud, often by organised gangs across the world, were costing the company at least $475 million a year.

Lawsuit over message axed

A judge in San Francisco, US, has thrown out a lawsuit brought by a couple who were accused in an Internet message of ritual sex abuse of children.

Michael Aquino and his wife Lileth sued Internet service provider ElectriCiti for carrying the offending message.

They said in the lawsuit that they were the victims of false accusations by an Internet user who had harassed, stalked and threatened the couple for more than a year.

But Superior Court Judge David Garcia said that federal law gave ISP protection from the actions of third parties and dismissed the complaints.

The lawsuit was one of the first following the 1996 federal Communications Decency Act, which aims to protect ISP from liability in such cases. The legislation says: "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."

Court action over porn CD-ROMs

A man in the US used the Internet to sell pornographic CD-ROM software in Japan, a court heard.

Yasuaki Hashiro, 34, from Japan, advertised the CD-ROMs on the Net while in New York and then received orders by e-mail, receiving a total of 200,000 yen.

He was arrested in April when he returned to Japan and has now been given a year in prison, suspended for two years by the Hiroshima District Court.

Judge Sumiko Ikemoto said in a ruling that although the crime was vicious, Hashiro had already received social punishment by resigning from the company he worked for.

Conference on Net crime

Law enforcement groups trying to police the Internet face considerable problems, a conference in Canada was told.

The three-day meeting in Toronto on Net hate featured speakers from law, government and business and tried to pin down the best way to keep the Web legal.

A spokesman for Canada'a largest province, Ontario, said that Internet service providers should be held responsible for objectionable material that is made accessible to Canadians.

Michael Bernstein, deputy director of prosecutors for the Crown law office, criminal unit of the Ontario Attorney General's ministry, said: "Hate propaganda is a poison, and anyone engaged in a commercial enterprise has to protect their customers from poison to the best extent possible."

He said that international boundaries posed a problem in prosecuting propaganda and pornography on the Internet, although he added that existing laws could still be used in many cases to combat the threat.

But Jim Mercer, a network specialist, told delegates that Internet service providers were like telephone companies, and could not be held liable for what their customers got up to.

He said: "There is not much we can do which isn't just a facade. The best tool against it is to teach people not to listen to it, to rebuff it.

Computer crime needs new policing

Police in the United Arab Emirates need new techniques and technology to step up the fight against computer hackers.

Hisham Farid, of the Faculty of Sharia and Law at Emirates University, said that the police should recruit experts in the field and called for existing laws to be updated to take into account the latest developments in cyber crime.

He said that the lack of physical evidence often posed problems for law enforcement groups and that evidence such as electronic data was not admissible in courts of law under the current legislation.

Mr Farid said: "Information is an abstract item that cannot be treated in the same way as murder and robbery.

"There is no law forcing witnesses to reveal the codes or passwords or the key to the systems that might, for any reason, be subject to police investigations."

He said there was a need for police forces across the world to co-operate in investigations because computer crime, especially on the Internet, crosses all geographical boundaries.

Attack follows e-warning

Police in Dubai are investigating an attack on a man who received an e-mail warning threatening him.

A police statement said that an American woman had been arrested on a charge of causing an assault and the incident could be the first Internet crime of its kind in the Gulf emirate.

The statement said that the woman met the victim, a Lebanese national, at Dubai's Internet cafe and asked him to stop making complaints against other Net users.

And the next day a man told the victim not to harass the woman or send any messages to her. Two days later he received an e-m which said "Watch out for yourself...this the last warning".

Later the Lebanese man was assaulted b five men causing multiple injuries.

Combating cyber crime

A special task force is being set up i Taiwan to crackdown on the growing problen of offences committed using the Internet.

The police will team up with experts fro the communications and economic ministrie to fight any illegal activity on the Net, rangin from illegal firearms to pirated software.

Justice Minister Liao Cheng-hao sai "The growing frequency of criminals usin the Internet to find buyers, together with frau and crimes against the Internet users, hav prompted us to set up."

Recently a graduate student was arreste in Taiwan after he set up a site on the We with instructions on how to make bombs fro fireworks. And a week earlier a teenager wa arrested for running a site called Firearm Godfather that offered handguns for sale.

The Net page is registered in the US an offers Beretta pistols at $2,500 to people i Taiwan.

Serial killer web page axed

Service provider America Online ha stopped carrying an Internet page created b a journalist who specialises in covering seria killers.

The page included the unedited writing of three serial killers and a DIY "self start seria killer kit" written by Keith Jesperson, a ma who killed eight women.

Sondra London, 50, who calls herself th "queen of the serial killer journalists" set u the pages and says she has now received a least 50 offers to put the information back u elsewhere on the Web.

She said: "I'm so excited. My enemie have made me famous beyond my wilde dreams.

"I'm not sponsoring any kind of school or serial killers. I know enough about this ind of diseased mind to know that the ideas hey have arise spontaneously. They're not ormed by suggestion."

Reservations over Indian gambling

The state of Wisconsin in the US is suing a communications firm over its deal with an Idaho native tribe to stage a lottery on the Internet.

In the lawsuit, the state attorney general alleges that Executone Information Systems is breaking state anti-gambling laws.

Executone, based in Connecticut, has the exclusive rights through its UniStar Entertainments subsidiary to run the National Indian Lottery and company president Alan Keesman says the case has no merit and that the firm is entirely legal.

He said: "UniStar and the tribe intend to vigorously defend the rights of the tribe under the Indian Gaming Regulatory Act to offer the US Lottery to consumers accessing the Internet site from Wisconsin."

Phone fraudster faces imprisonment

A computer studies graduate could go to jail after he admitted his part in a multi-million pound Internet fraud.

Omar Flatekval, 23, from the UK, hacked his way into computers at the American Telegraph and Telephone Company, copied details of telephone charge cards and sold them on using the Net.

The fraud is estimated to have cost AT&T $17 million and bogus charges of up to £10 million were run up on its customers' cards over three years.

Investigators found 61,500 calling cards logged on to Flatekval's computer system and it is thought that he made around £50,000 in the scam.

Flatekval admitted conspiracy to defraud when he appeared at Newcastle Crown Court and he will be sentenced at a later date.

Paedophile networks

The National Crime Authority in Australia is reported to have identified loose networks of up to 5,000 paedophiles across the country.

Compiled using state and federal databases, the report lists those who have sexually abused children and trafficked in pornography and it has now been distributed to government and law enforcement agencies.

It called for a national intelligence project to examine the level of use of the Internet by paedophiles and called for more police resources, training and technological resources to monitor computer pornography.

Megan's Law online

The names of dozens of Los Angeles' worst sex offenders have been published on the Internet by a self-styled anti-crime crusader.

Nearly 100 high-risk paedophiles are listed in the site, and more will be added using information from Megan's Law, which pinpoints the whereabouts of 64,000 convicted sex offenders in California. The law was named after seven-year-old New Jersey girl Megan Kanka who was killed by a paroled molester, and the information has until now only been available on CD-ROM to a few police agencies.

The site has been set up by Ken LaCorte, who says the public have a right to know if there is anyone who could pose a threat to their children living in the neighbourhood.

He said: "When they keep that information under lock and key in police stations, thousands of these men will be getting closer to children."

State authorities said they had tried to keep the information from being too easily accessible in case it was used by paedophiles to establish closer links and to prevent any reprisal or vigilante attacks.

Critics of the web site warn that putting such emotive material in an unregulated place such as the Net is dangerous.

Elizabeth Schroeder, associate director of the Southern California American Civil Liberties Union, said: "The possibility of hacking or fraud or simply mis-keying the information makes this an extraordinarily dangerous way to play with people's lives."

Members of the public were also able to search the entire CD-ROM themselves at a special booth at the Los Angeles County Fair, with an estimated 10,000 people looking to see if any paedophiles might be living nearby.

Spam spurned by Net provider

A Tokyo based Internet service provider has filed a ground breaking lawsuit in the US in an attempt to stop a Los Angeles firm from flooding it with unwanted ads.

Typhoon Inc has taken the matter to the District Court after the LA company Paging America allegedly deluged it with unsolicited mail, known as spam.

The lawsuit says that Paging America, which sells pagers, engaged in a massive e-mail advertising campaign in March and May this year and that false addresses were used.

Typhoon legal counsel Andrew Mansfield, of Internet law firm O'Melveny and Myers, said: "The Internet is not a playground for pirates and scam artists.

"The defendant's unlawful conduct nearly crashed Typhoon's system and thousands of America OnLine customers were lead to believe the spam originated with Typhoon.

"Lawsuits like this represent the cutting edge of efforts by legitimate businesses to curtail Internet imposters and free-loaders."

He added: "This suit does not seek to prohibit honest spamming, annoying as such messages are to most Internet users. The defendants weren't willing to put their own name and return address on their unsolicited messages or even use the server of their own Internet service provider. Spam isn't the issue. Illegal conduct on the Internet is."

Typhoon says that any unauthorised access to its e-mail server violates the US Electronic Communications Privacy Act and was a trespass and misappropriation of its property. It also says that putting false addresses on e-mail also breaks the law and that associating the firm with spamming constitutes libel under Californian legislation.

• On July 8 this year, the state of Nevada passed a law requiring $10 damages per item of commercial, unsolicited e-mail and several bills have been introduced in Congress to address the problem of spamming.

Junk e-mailer allowed to stay

One of the leading senders of unsolicited e-mail must have its Internet access restored, a federal judge in the US has ruled.

Cyber Promotions Inc sued Internet service provider Apex Global Internet Services Inc after its Net account was terminated.

District Judge Anita Brody ordered Apex, also known as Agis, to reconnect the service because of a 30-day notice clause included in the contract and Cyber now has until October 16 to find a new service provider.

Judge Brody wrote in her report: "Many computer users find the receipt of bulk e-mail annoying and intrusive.

"However, the fact that Cyber is an unpopular citizen of the Internet does not mean that Cyber is not entitled to have its contracts enforced in a court of law or that Cyber is not entitled to such injunction relief as any similar business."

Cyber Promotions was allegedly behind a large volume of unsolicited e-mail, known as spam, with thousands of customers paying the firm to send up to 20 million junk messages each day.

At the time of the initial termination in September, Agis said: "Outstanding security issues are the reason Cyber Promotions was disconnected from our backbone.

Child porn on the Net

Delegates to a conference were told that up to 27,000 people access paedophile pornography on the Internet every day.

The Psychological Society Conference in Cambridge, UK, heard that many of these users swap obscene pictures and stories ranging from so called snuff videos to pictures of naked children who were offered up for abuse.

Members of the society were told that the Net provided a detailed list of paedophile fantasies which were presented as normal interests and that people with only marginal interest in the material could be drawn in by the ease of hooking up to cyberspace.

Net fraud watchdog goes online

The National Consumers League in the US has launched a service to monitor and fight back against Internet scams which cost millions of dollars.

It has set up a Web page to list the top ten Internet frauds and help warn users about such online problem areas as pyramid schemes, business opportunities, credit card offers and product sales.

The group says Net fraud was up by 300 per cent last year and looks set to rise further as people get enticed into too-good-to-be-true schemes.

NCL president Linda Golodner said: "Our new Web pages give tips on how to protect yourself from fraudulent deals. Cybercrooks are in your wallet with a click of the mouse.

"Consumers must watch for common signs of fraud such as extravagant promises of profits, guarantees of credit regardless of bad credit history, and incredibly low prices or prizes that require up front payments."

Charter could protect standards

An international charter could be drawn up to deal with questions about illegal content, encryption and data privacy on the Net, a conference was told.

The European Union's telecommunications chief Martin Bangemann told delegates at a meeting on Internet standards in Brussels that he was looking for general principles to be set out.

He said: "The idea is it should be very flexible, but at the same time trying to find the basis for common positions." He added that a body could be set up to help implement this: "I personally believe that at the end of the day we should have somebody who could act as as a clearing house who would be the to help other people with practical problems

A spokesman for President Clinton sa that the US might be willing to support such move, so long as it met specific requirement

Ira Magaziner, Clinton's Internet polic expert, said: "We think there needs to b international understandings on a variety (issues - some of which may need to be form agreements, some informal understanding and common approaches. If that is what meant by a charter, then I think we would b very interested."

He added that Washington differed fro the EU on how to protect the privacy (information carried on electronic networl and that codes of conduct were needed rath than legislation. He said: "Industry regulatio we believe, will not stifle the Internet, but will be more effective in regulating privacy

But Luxembourg Communication Minister Mady Delvaux-Stehres feared th this would not be a comprehensiv solution.She said: "I don't believe we ca solve all problems with self-regulation."

Bootleg software

Authorities in Mexico seized the large haul of pirated software since a new la protecting copyright came into effect.

Microsoft, Lotus and Adobe, as well a other large name software suppliers, ha complained that the country was bein flooded with illegal software.

Police raided a market in Tlalnepantla, suburb of Mexico City, and took 4,00 computer programs and 17 computers, wit four people being arrested.

California crackdown on Net abusers

Lawmakers in California, US, hav clamped down on paedophiles who use th Net to lure in unsuspecting children.

The bill makes using the Internet o e-mail to distribute certain material t youngsters punishable by a jail.

State Governor Pete Wilson, in signin the law, said that FBI figures showed that ther vere 1,700 cases of sexual material being ansmitted to minors in 1994, the most recent tatistics available.

He said: "Paedophiles have used the infettered access of the Internet to wage open var on our children. This bill gives law nforcement and prosecutors a powerful veapon to use against sexual predators who rowl for victims online."

California law already makes it a crime o use the telephone to attract a minor, although nder the new law Internet service providers re not responsible for the criminal misuse of he Web by any of their customers.

Free legal help on the Net

Basic legal information is being published on the Internet covering the most frequently asked questions.

Compiled by experienced lawyers, the site contains thousands of pieces of advice covering dozens of legal topics, including bankruptcy, accidents, divorce, business, tax and trademark issues.

The Net pages are US-based and apply to American laws, although countries elsewhere may get some benefit.

The site's creator, Gerry Goldsholle, said: "Free Advice is proud to be educating Americans about their legal rights and responsibilities. Now ignorance of the law really isn't an excuse."

The Web address is http://FreeAdvice.com

Auditing CD-ROM

Software piracy watchdog the Business Software Alliance has launched a free CD-ROM that helps firms come clean about their programs.

LegalWare provides a step by step guide to the auditing process as well as a directory of tools available on the market, with details of many software firms' packages and licensing conditions included. Information is given on the different types of theft, including copying, counterfeiting and Internet piracy and there is a guide to the copyright laws in both the UK and Europe.

Clare O'Brien, director of marketing for BSA Europe, said: "Legalware is quite simply the most comprehensive information tool available for companies who want to ensure that their software is fully licensed and it will hopefully act as a spur to those who take the issue less seriously. Software theft has become an endemic feature of business life."

Scam sites targeted

The UK has joined an international campaign to fight con merchants on the Internet.

Civil servants spend hours every day scouring sites for fake get rich schemes and warning the operators by e-mail.

Officials from 30 other countries are also involved in the operation, which was started by Australia's consumer protection watchdog.

Ian Blomfield, of the UK's Office of Fair Trading, said: "The idea of this was to heighten awareness of the issues internationally. It's true we will only reach a small number of the kind of sites offering these scams, but with all of our counterparts acting simultaneously across the world, we hope to have made an impact."

Scrambling report

The European Union has urged governments across the world to take a hands off approach to controlling encryption on the Internet.

EU Telecommunications Commissioner Martin Bangeman said that strict controls would penalise law-abiding users rather than the criminals they were targeted at.

And he said that the US, which restricts exports of the strongest encryption technology, was becoming isolated in its approach.

"We must engage in a debate with the Americans at an international level," he said.

Mr Bangeman was speaking as the EU published a report on how it should promote Internet security, which proposes legislation on so called digital signatures in the first half of 1998. The law would address issues such as legal recognition of signatures, liability, technical requirements and certification authorities which would confirm individuals' identities.

Mr Bangeman added: "It's not possible to prevent criminals from using modern technologies in order to protect themselves and their messages from the police. There's not much point in preventing legal users from access to this."

Encryption is at the centre of debate because some governments and law enforcement groups fear it could be abused if it got into the hands of criminals and France has already virtually outlawed the use of encryption software.

But the EU said controls could hinder the growth of the technology and create problems in doing business over the Internet.

Pennsylvania law

Using the Net to try to lure children into sex acts will carry heavy punishments under a bill passed in Pennsylvania, US.

Under the bill, state authorities can prosecute anyone in the country who illegally contacts children living in the state and sentences include up to five years in prison or a $10,000 fine.

Bill sponsor Matthew Baker said: "These predators are clever. They pretend to be a member of the child's peer group, establish trust through a series of contacts with the child, and then either go visit the child, lure him into running away from home or kidnap him."

Currently 13 states in the US have laws to prosecute paedophiles who use the Net.

Call to fight porn

One of the leading figures in Internet specialists said Germany's campaign to combat online pornography and propaganda is a basic right.

Michael Dertouzos, director of the influential Institute for Computer Sciences at Massachusetts Institute of Technology, said he did not see the country's attempts to fight objectionable material as an attack on free expression.

He said: "My belief is that countries should preserve their cultures. We have trade and criminal law cross-national laws on the Internet."

Product News

Smart cards

Smart cards are being used to fight back after the Russian mafia ambushed wage vans and stole oil workers' wages in Siberia.

ICL has developed a system where workers can pay for services using an intelligent card fitted with a microchip to reduce the risk of losing hard cash.

Russian oil giant LukOil used to be at the mercy of gangs who attacked workers or delivery vans on payday.

Smart card consultant to ICL Denise McDonald said: "Often oil workers are in the middle of nowhere and carrying hard currency is risky. The cards have been developed for areas where there are poor telecoms structures."

ICL has also sold its system to clients in Nigeria and the US and can be contacted on the Internet at http://www.itc.icl.ie/products

E-mail virus detector

The threat of e-mail viruses infecting computers hooked up to the Internet has prompted many users to take emergency action.

US firm Trend Micro Incorporated says it has found a huge market for a program designed to weed out infected e-mail files before they can cause any damage.

The company's InterScan VirusWall scans e-mail attachments, http Web downloads and ftp file transfers and is also claimed to block Java applets and software not recognised as coming from an authentic supplier.

Trend Micro's president Irfan Salim said: "Unfortunately e-mail attachments are the greatest virus threat to most corporations due to the rapid spread of macro viruses and the lack of tools to detect viruses in this environment."

The software is currently available for Windows NT, Solaris and HP-UX operating systems

Network protection

A system has been developed to act as a burglar alarm to warn of security breaches in computer networks.

Network General Corporation has launched CyberCop which it says will protect against both internal and external attack and performs real-time surveillance of network activities.

CyberCop is placed at key locations throughout a network and the sensors analyse the data throughput, looking for anything suspicious. If a problem is found, evidence is recorded in trace files which can be recalled to show the exact breach of security.

Nancy Blair, director of product development at Network General's Internet business unit, said: "Our customers perceive a growing threat to their business operations.

"Many companies are experiencing a significant increase in the number of attacks against their networks.

"While the threat from internal users or intruders masquerading as trusted insiders has not diminished, the number of external attacks is growing due to widespread Internet use."

Once CyberCop detects an anomaly, it alerts managers through e-mail, paging messages or screen prompts and its makers say the system complements other security systems such as firewalls and encryption.

Contact Network General at (US) 650 473 2000 or on the Web at http://www.ngc.com

Cyber porn on business computers

A firm of computer detectives has found that a quarter of computers contain pornography of all kinds, including some cases of hard core material involving children.

Digital Detective Services, a US computer forensics and investigations company, said that many businesses were completely unaware of the level of misuse being conducted by employees.

Sudeep Bose, director of investigations and a specialist in the field of corporate computer policy development, said: "The results are not startling. Many small and medium size firms have no formal policies or standards on Internet use or materials transmitted on-line.

"Employees are left to police themselves and that does not work. We commonly find persons using corporate networks to view illicit materials. At best this is a waste of corporate resources - at worst, depending on the materials, it is a crime.

Mr Bose added: "Employees with tainted materials on their computers are usually terminated immediately. Employers despise the possibility of exposure and other issues which readily arise from these situations."

The results of the study come from data accumulated by DDS over 11 months and 150 individual investigations.

Dan Bender, manager of operations, said "Executives call us to analyse what an employee has been doing with the computer."

"When we present our findings, they are usually shocked. An employee being investigated for releasing trade secrets turns out to be a collector of on-line pornography It really stirs up office politics."

And DDS has found that while most of the misuse is fairly minor, those users with some computer knowledge will often try to hide their activities.

"Many employees try to delete files and clear caches when they suspect they are being investigated for anything," said Amadali Arabshahi, director of IT.

"We have the technology to restore deleted files and view hidden or password protected data. No bit of information is left unturned."

Digital Detective Services is located in Falls Church, Virginia and can be contacted on (US) 703 575 9326.

New analysis software

A suite of analysis programs is aimed at helping police and investigators collect and sift through vast amounts of case information.

The Harlequin Group says the Harlequin Intelligence suite supports law enforcement agencies around the world and lets them store data and trawl through it to pinpoint suspects in crimes and collate evidence.

At the heart of the system is Watson, which lets investigators import, track and interpret data from a wide range of sources, and then the software can identify links and reveal associations that might not otherwise be found.

Its makers say that the suite is designed to handle a large range of crimes, from murder and fraud to drug-related offences and counterfeiting.

The system requires a PC running

Vindows 95 or NT.

For more information contact Harlequin t (US) 617 374 2555

Java security

A system designed to protect networked computers against malicious use of Java and ActiveX applications has been launched by JS firm Finjan.

SurfinCheck for NT operating systems works by scanning Java applet headers and letecting potentially damaging behaviour, while allowing safe programs to carry on running.

Chief executive officer of Finjan Software Shlomo Touboul said: "Priced cost-effectively, SurfinCheck ensures that quality Finjan technology is applied appropriately and affordably to the needs of small and medium-sized businesses using the Internet.

"Every type of business, from a law office to an Internet security provider, can now easily surf the Net protected.."

Finjan says that the use of Java and ActiveX on the Net means anyone seeking to maliciously manipulate corporate information or attack business computers can do so much more easily.

Mini applications like Java applets enter network computers whenever users access the relevant enabled web sites and this means unchecked programs can enter into networks without any warning.

SurfinCheck costs $695 and Finjan can be contacted on (US) 408 727 8120, e-mail info@finjan.com or the web site at http://www.finjan.com. Free 30-day evaluations of SurfinCheck can be downloaded at http://www.finjan.com/products./html/surfincheck.html

Secure mail delivery for Macs

Internet document delivery firm Tumblweed Software Inc has launched a system for Macintosh computers which it claims allows immediate and secure communication.

Tumbleweed Posta Symbol Times works regardless of which e-mail server a business has in place, and its makers say it is not necessary to overhaul the company's existing network.

When documents are sent they arrive intact with no loss of formatting or unwanted changes due to conversions and users can track the delivery of material.

David Coursey, an industry expert, said the system made a useful contribution to Net security. He said: "E-mail will never work perfectly. There will always be files that get mugged. If you're a law firm, this makes a lot of sense because it gives you security all the way. You can now e-mail documents that are paper perfect, and it's secure the whole way through."

The system for the Mac costs $3,999 for the server, which includes up to 20 licenses. Tumbleweed can be contacted on (US) 415 369 6790 and its website is http://www.tumbleweed.com.

Credit card thieves targeted

A software company in the US is combating fraud by using a system which examines the spending profiles of credit card users to spot problems.

HNC Software, based in San Diego, helped develop technology for the US Department of Defense and is now using similar ideas to attack fraud and counterfeiting.

In its military use, the software recognises the visual profiles of potential targets and allows pilots and troops to fire in the direction of an enemy and depend on the weapon to find the target itself.

The civil system, called Falcon, works in a similar way by comparing card transactions to a model of typical fraudulent spending patterns and a historical profile of the cardholder's purchases over recent months.

One example its makers gave was when a woman filled up her car with petrol her credit card was counterfeited and used by the criminal to buy petrol in another service station nearby. But the Falcon system worked out that it was unlikely that the woman would need petrol so soon after filling up the first time, and flagged the fraud up to be investigated.

Falcon was on display at the American Bankers Association's Bankcard Conference in Long Beach, California, where the issue of the growth of fraud and crime using the Internet and computers was one of the central topics.

Susan Sylstra, executive director of the International Association of Financial Crimes Investigators, said: "The crooks are computer literate too. We've got to be at least as fast or faster than the ways the crooks are getting their information around."

Security and virus protection

A system which offers PC access control and security while tackling viruses has been launched by IT consultant MIS Europe Ltd.

SmartLock is available in two versions - SmartLock BAS and SmartLock PRO and SmartLock Net provides centralisation of maintenance and supervision of network operations.

The system monitors access to PCs to prevent tampering with important data and hard disks are automatically and transparently encrypted.

It also generates electronically marked and encrypted floppy disks that allow the controlled sharing of data and software within user groups. And the system selectively restricts access to both local and LAN hard disk areas, stopping individual files or entire directories from being opened by other people.

SmartLock automatically records the use of software and peripherals and supplies regular reports on user action and it uses "stealth boot" technology to protect hard and floppy drives which takes control of the PC before the operating system is loaded.

Managing director of MIS Europe Mark Mottershead said: "The progressive distribution of information to PCs has not been accompanied by a parallel progress in security procedures.

"There is a high risk to sensitive data due to operating errors, deliberate attacks on information systems, viruses, tampering, thefts and accidental loss of data. These are all very real dangers and threaten the very existence of a company."

The system is compatible with Windows 3x and Windows 95 or DOS 3 or above.

MIS can be contacted on (UK) +44 (0) 1622 723400

Rent a hacker

A firm in Florida, US, is offering security consultation services, including legal hacking, for companies that have or think they have flaws in their systems.

Winn Schwartau, chief executive officer of The Security Experts, said: "People need to realize that their businesses today are based on technology and most do not understand that technology.

"We go in, analyse their processes, their business functions, determine what fixes are appropriate to the business, and either fix the problem for the company or help them fix the problem themselves.

"We prefer to help companies work out a process where they can themselves anticipate and heal vulnerabilities in their systems."

The firm provides commercial consulting services to mid-to-larger companies that do business on the Internet, or are actively involved in electronic commerce, companies that need to secure their electronic assets from internal or external attack.

Mr Schwartau said that the programme is tailored to specific client needs and rules, so that investigators do not go too far.

He said, "If you, or any company, don't want us to go so far as to extort employees, or if you don't want us to do background investigations on the staff to find their vulnerabilities so we can exploit them, it will be written in your set of rules. We will only go as far as you want us to go to find answers."

He said his experts might pretend to be international criminals, internal embezzlers or even terrorists.

"The amount we 'steal' from you doesn't matter - $5, $5 billion. If we can get in, we can get in. In order to protect against the bad guys you need to be able to think like the bad guys."

For more information go to the Web page at http://www.infowar.com or telephone +1 813 393 6600.

Company Merger

Two firms based in the UK involved in data recovery and evidence retrieval have merged.

Authentec and Vogon are now known as Vogon International Limited.

The new firms says it brings together the specialist skills and resources from both companies.

Vogon International Limited can be contacted on tel: +44 (0) 1869 355255.

Fingerprint system speeds up police work

Police in New Jersey can process criminals far quicker using a specialist electronic fingerprinting system.

US firms Identix and Morpho Systems have teamed up to produce the Fully Integrated Fingerprint Identification System, which will now be installed in eight cities in the area.

New Jersey State Police Sgt Philip Boots, who heads the automated fingerprint department, said the system would process about a quarter of the state's annual number of criminal arrests.

He said: "We see several advantages in turning from traditional ink fingerprinting to the Identix system.

"In addition to the overall greater accuracy and speed in booking a suspect, our initial experience shows that the entire procedure takes less than ten minutes compared with as many as 11 days under the old method."

Fighting phone fraud

A system has been launched in the US to tackle the huge problem of mobile phone misuse.

Wireless telephone fraud costs an estimated £1 billion dollars a year, with about 30 per cent of this from roaming fraud where users move from cell to cell.

Firms T-NETIX and GTE TSI now offer the system for use by telecommunications operators beat the thieves.

A spokesman for GTE TSI said: "Our FraudForce services offer wireless providers the knowledge and means to manage their roaming traffic.

"With Voice Verifi-Air we can now significantly enhance the security of the verification process while providing a more user friendly interface."

For more information contact T-NETIX on +1 303 7909111

Sybase technology fights crime

Computer solutions firm Sybase has announced it is helping to develop a system for the state of Colorado in the US to catch more criminals.

The firm is setting up a communications infrastructure that lets all of the state's criminal justice agencies share real time information so they can work more efficiently.

And the Colorado Integrated Criminal Justice Information System is the first of its kind that lets individual bodies push and pull data from their colleague agencies.

Chairman of Sybase Mitchell Kertzman said: "By facilitating the flow of information across state and local agencies, we are providing officials with powerful weapons to fight crime."

CICJIS will establish an integrated computer information system which standardises data and communications technology throughout the primary criminal justice community. This includes law enforcement, district attorneys, state funded courts and state funded correctional facilities.

It will also allow tracking the complete life cycle of a criminal case through the various stages.

David Usery, in charge of the CICJIS task force, said: "Inter-agency collaboration is enhanced in a fast and cost-efficient manner.

"It streamlines the communications process without requiring vast expenditures on new computer software or hardware."

Public sector analyst Lesley Kao said: "Governments will watch the CICJIS project closely as this provides a previously unseen option for jurisdictions to make use of existing systems and investments. The ultimate benefit is that they will be able to provide better service to their citizens."

The system is expected to go on line in mid January of next year.

Economic crime conference

Delegates to a conference were warned that a new breed of fraudsters are using new technology to steal vast quantities of money.

The Symposium on Economic Crime in Cambridge, UK, was told that computers and the Internet were fast becoming popular tools for criminals.

About 900 delegates attended, including detectives, Internet companies, customs officers, government officials, lawyers and academics. Among the subjects discussed were the growth of electronic banking and the potential for fraud, money laundering, online gambling, electronic evidence and international cyber crime.

The theme of the conference was the globalisation of criminal activity and the associated developments in technology in terms of risks, control, prevention and enforcement.

One of the organisers said: "If the law has not been able to keep up with the internationalisation of crime, in either its reach or its resources, the prospect of criminals and in particular organised crime, moving into cyberspace is fundamentally more threatening.

"Developments in technology have in effect created a global business community. Criminals have of course followed suit and in some instances, given their resources, outstripped their law-abiding competitors.

"Added to this is the threat of destabilisation of systems and the integrity of data, for subversive or belligerent purposes. The prospect of crime and warfare in the realm of cyberspace is today a reality."

Philip Rutledge, deputy chief counsel at the Pennsylvania Securities Commission said: "Once again, fraudsters have adapted to new mass technology by transferring their schemes to the Internet.

"While the Internet has some drawbacks similar to the newspaper, advantages of instantaneous communication to millions of people, availability of e-mail and construction of very legitimate-looking Web pages and links overcome these disadvantages.

"Like the transition from the newspaper to the telephone, financial regulators are faced with adapting to new methods of communication.

"The Internet offers some significant problems and some opportunities for financial regulators."

Mr Rutledge said that there were many hurdles in the way of reducing the fraud. He said a generation problem meant younger people understand the medium better than older ones, but the older generations were generally in charge of regulation.

But he said that the Net also gave the chance for governments to give information of those convicted of similar frauds and publish them for all to see on the Net in an attempt to educate users.

"Criminals have outstripped their law-abiding competitors"

Rosalind Wright, director of the UK Serious Fraud Office, stressed that the laws and regulations governing computer misuse should be adapted and improved to keep pace with innovations.

She said: "We must never allow the technology to race ahead so that the law is limping behind to catch up. Internet fraud is one aspect of the increasing internationalisation of economic crime.

"London is, of course, the biggest international financial centre in the world and the biggest foreign exchange centre.

"Consequently it is crucial that the UK leads the way when it comes to the regulation of financial markets and the criminal process for fraudsters."

She added: "Fraudsters exploit territorial boundaries and differing legal systems to make the process of investigation and prosecution more complicated and difficult."

And she called for a more streamlined approach to dealing with major fraud in the UK, along with the need to persuade banks and financial centres to co-operate with investigating officers by disclosing privileged details of suspects.

Academic Ernesto Savona, a director of the crime research group at the University of Trento, Italy, told the conference: "Traditional areas such as drug trafficking are becoming too risky. Economic crime is more profitable and less risky."

Corrado Conti, the director general of Italy's stockmarket watchdog group Consob, said the Internet posed problems for the world's financial institutions.

He told the delegates: "It is the responsibility of the market regulators to evaluate the trade-off between the degree of freedom in the use of new technologies, and the possibilities that the same technologies may have negative repercussions on the integrity of markets.

"Legislation can no longer be left to the individual national authorities and regulators. International co-operation arrangements will eventually lead to the creation of common surveillance procedures."

Representatives from the European Union said that the difficulty police forces faced in investigating cyber crime and fraud would be likely to increase further.

"We are under no illusion that fraud will go on and as we close one loophole, another will open up," European Commission deputy financial controller Alan Pratley said.

One of the organisers, Professor Barry Rider, director of the Institute for Advanced Legal Studies, said: "Law enforcement agencies have hardly managed to get a grip on the conventional criminal who is able to flit from one jurisdiction area to another utilising foreign nominees and banks to hide his ill-gotten gains.

"Add the cyber dimension and the fight becomes even more one-sided. The implications for money laundering are profound, but so are they for the stability and integrity of the financial markets and banking generally.

"No one knows the true extent of computer related or aided crime, let alone the incidence of electronic sabotage and subversion."

The Symposium also included a separate programme focusing on the special issues and concerns in South Africa, especially the problem of money laundering and how to combat it.

- A full set of symposium papers will be published by Kluwer Law International.

Paedophile dragnet

A huge clampdown on Internet child pornography by US authorities has resulted in more than 1,500 suspects being targeted worldwide. Paul Johnson looks at the remarkable operation and examines its success so far.

The message from New York State Attorney General Dennis Vacco is stark: paedophiles using the Internet will be hunted down and prosecuted.

Vacco has been at the forefront of a concentrated campaign over the last few years to take a pro-active role in policing the Net and ferreting out those who misuse the technology for peddling pornography.

Over the last 18 months, a joint sting operation first launched by Vacco has uncovered child porn traffickers throughout the US and also in the UK, Switzerland and Germany.

So far the joint federal and state dragnet has resulted in more than 120 court case referrals and at least 31 convictions, with more to come.

And the sweeping probe, called Operation Rip Cord by Vacco's investigators and the Tholian Web by the US Customs Service is already thought to be the most successful operation of its kind anywhere.

Law enforcement agencies found more than 200,000 child porn images on $137,000 worth of computers they seized. Investigators used standard techniques coupled with state of the art technology to retrieve the evidence.

Vacco said the sting "cracked the code of cowardly child pornographers and enabled us to follow their tracks and nab them in the act."

He added: "With these prosecutions, we have put child pornographers on notice that New York won't ignore this illegal activity, which threatens the safety of our children.

"This is a tremendous leap forward in our battle to protect children from exploitation by child pornographers and holding accountable those responsible for peddling and profiting from this despicable trade.

"As the father of two young boys myself, these pornographic images are too disturbing to describe."

The undercover probe team, made up of Vacco's investigators and Customs agents, posed as potential paedophile trading partners to lure suspects into online conversations to trap them. In a dramatic demonstration of how easy it is to get access to the illegal pictures, investigators in an Internet chat room were approached by another user offering a picture of a nine-year-old girl involved in an incest assault and within 10 minutes the photograph had been sent through.

One investigator was said to be so disgusted by what he saw that he ripped a computer plug from the wall, and another said the images were so disturbing that he had trouble sleeping at night for several weeks.

And even more worringly, Vacco said, many of the 200,000 images seized appeared to have been created recently, which he feared pointed to a "resurgence of victimisation" of children. He said that the investigation's goal is to "protect kids, not to go after people exercising their First Amendment rights. In the end, these are not victimless crimes."

New York State Police Superintendent James McMahon said: "This investigation revealed, not only the relative ease with which investigators can obtain child pornography, but also how far and wide the problem of Internet child porn distribution really is."

Vacco said that America Online, the nation's largest Internet service provider, assisted in identifying suspected child porn traffickers who used its service.

In New York the sting has led to seven state prosecutions, including a college student training to become a kindergarten teacher, and one 21-year-old man in the Bronx was arrested and stands accused of using the principal's computer at a state school to send and receive illegal pictures.

Under New York State law, transmitting child pornography over the Internet is punishable by up to seven years in prison and obtaining such pictures and storing then on a computer carries a maximum sentence of four years in jail.

Vacco has vowed that the investigation will continue and that more arrests and court cases nationwide will follow and he added that an Attorney General's Internet and Computer Unit has now been set up to directly tackle the problem.

As chairman of the nationwide taskforce to quash child porn on the Internet, Vacco will hold talks with representatives of Attorney General's offices of all 50 states to discuss strategy and techniques.

He said: "I want to forge lines of communication that will allow us to trade leads into this perverse crime.

"My investigators and prosecutors will have the opportunity to pass on the methods we have been able to successfully use against Internet sex predators to the other states.

"Since Internet sex crimes frequently cross over state lines, co-operation between law enforcement officials is imperative."

And Vacco hopes people will take advantage of a cyber crime tip line which puts users in direct contact with the new Unit to alert the office of suspected fraud or criminal activity on the Web.

Vacco said: "The Internet presents a vast frontier for scam artists and con artists, as well as paedophiles and other criminals. Now, with a single mouse click, Web users can notify my Internet Bureau of suspected consumer or investment fraud, or even to report Web sites that traffic in illegal drugs, child pornography, or pitch tobacco and alcohol products to minors."

The tip line, which Vacco said was the brainchild of Long Island state Senator Owen Johnson, can be accessed from Vacco's home page at http://www.oag.state.ny.us on the World Wide Web.

The Web site, recently cited by the New York Law Journal as among the most useful government sites, received over 22,000 hits in its first month of operation Vacco said.

Senator Johnson first proposed the tip line idea to the Attorney General shortly after voting in favour of new funding for the Attorney General's Internet unit.

The New York City-based unit is headed by Assistant Attorney General Eric Wenger.

A non-technical problem

Not all of the problems involved with investigating computers are technical ones. Jim Bates looks at the issues surrounding the implementation of computer forensic skills.

As an increasing number of police forces and other organisations become aware of the need for computer forensics, their immediate problem is how and where to get honest information about the growing range of products and services available in this field.

Deciding what is best for their particular needs and accurately evaluating what is available requires knowledge of the problem that they just do not possess. A common initial approach is to consult in-house specialists in their Information Technology departments or indeed anyone with the slightest claim to "computer knowledge".

Unfortunately, rather than providing the solution this can often make the problem worse because computer expertise (real or imagined) is one of the less important requirements when considering just how potential evidence on computers should be handled.

More important are detective skills, forensic awareness, knowledge of the Law and straightforward common sense. In a large majority of cases the evidence is only incidentally concerned with computing technology - blackmail letters, paedophilia, fraud and so on.

Of course there may be times when detailed expert knowledge is essential to a correct understanding of the value of evidential material but these are rare and must remain the province of the dedicated specialist just as in other forensic disciplines.

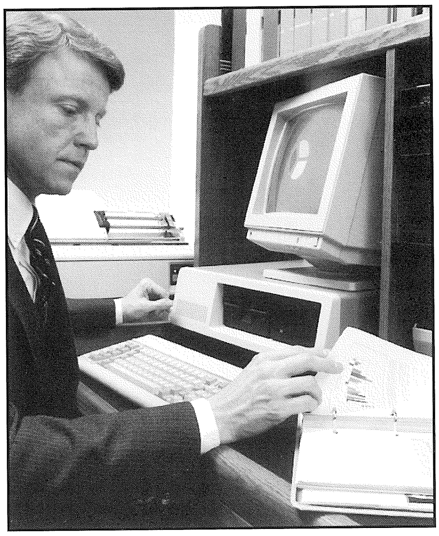
I have no wish to denigrate IT Managers or their staff, most of whom do a superb job often under difficult circumstances. It is a fact however that in just a few IT departments, particularly amongst personnel who may be poorly paid and badly qualified, there is a mentality which actively seeks to increase the mystique which still surrounds computer technology.

Most of us are familiar with these empire builders and can recognise their attempts to impress us with their knowledge. Sadly, some senior and middle managers tend to attach more importance to the word "computer" than they do to the word "forensic" even though parallels exist in other areas.

There is for example a world of difference between a Dentist and a Forensic Odontologist or a G.P. and a Forensic Pathologist.

In practice when an IT department is asked for assistance in evaluating forensic computing products and services one of two things will usually happen. They may indicate that they have no real knowledge of the field and are no better qualified than anyone else to evaluate or use any specialist equipment.

Alternatively they may seize the opportunity and begin looking for the most complex equipment with a maximum number of knobs, buttons, levers, dials, switches and gadgets.



Such equipment will obviously require more personnel and so the empire grows. There are a growing number of commercial sources for forensic computing equipment and some of them use questionable hard selling techniques which seek to exploit this "expert" mentality. So if a senior manager is tasked with the job of setting up a forensic computing facility, how is he to negotiate this minefield?

A reasonable approach might be to ignore the commercial sales pressures and begin by making contact with similar organisations who have already implemented such a facility.

They may tell of successes and failures; they may be able to highlight problem areas or suggest improvements or ways to avoid mistakes. In this way it should be possible to gain an accurate picture (warts and all) of just what is available and how best it can be used.

Detailed information concerning the less obvious questions of running costs and general efficiency can also be gathered along with a hopefully unbiased opinion about the integrity and technical support services of the companies involved. Such a process will help to build a knowledge base about what may be needed and what may be practical.

The next stage will be to invite chosen companies to demonstrate their wares.

Once again, the temptation to ask IT personnel to assist in technical evaluation should be avoided.

Much more important than the technicalities are the answers to questions concerning the company track record, case histories, user base, range of services, ongoing commitment, future plans and so on.

Do they undertake investigations themselves and if not, are they genuinely aware of the problems and needs of investigators? Where possible check case histories against court records, have a look at case reports produced by experts within the company.

A check with Companies House is also worthwhile - is the company all it claims to be? Is it healthy and expected to continue?

It is far more reliable to note the claims of competing companies and then check them with existing users than to simply take their word for it!

It is not suggested that any of the foregoing will be an easy process. All of the information gathered will need to be considered in the light of perceived requirements.

Will you need the flexibility of a general forensic capability or the more rigid strength of a dedicated department?

What are the projected staffing levels likely to be and how should they be costed?

One final point - it has been noted that in all cases where computer forensic facilities have been implemented, there has been an immediate and dramatic increase in the work load.

It is not thought that this will change, computers are a fact of life for all of us and that includes criminals too.

Jim Bates is president of the Institution of Analysts and Programmers in the UK

Court report

The UK has seen relatively few investigations and prosecutions of paedophiles who use the computers and the Internet illegally. But police forces are gradually becoming aware that technology can be abused and misused and that in any such crime there is a strong possibility that prime evidence can be retrieved from computer systems.

The recent high-profile case of Jean-Paul Hansford, which hit the headlines on television and in newspapers, shows that the whole legal system is beginning to address the situation and take the threat seriously. Paul Johnson reports.

In a ground-breaking court case, a man who had used the Net to peddle hard-core child pornography was jailed for 12 months.

Magistrate's son and radio presenter Jean-Paul Hansford admitted five counts of distributing indecent photographs of children and five counts of possessing pornographic images.

Hansford, 38, also asked for another 100 additional possession offences to be taken into consideration, covering a period from April 25 1996 to May 7 this year.

Bournemouth Crown Court, on the south coast of England, heard that Hansford, from the Isle of Wight, had resigned from his job as a breakfast show radio host at Isle of Wight Radio following his arrest on May 7.

When a forensic computer expert Peter Verreck looked at the contents of Hansford's PC, he found a total of 2,797 pornographic images and the court heard that Hansford had used the Internet to download the pictures and swap them with others on the global information network.

Some of the photographs were of youngsters aged as young as five or six being forced to take part in sexual acts, the judge was told.

Timothy Coombes, prosecuting, said: "Material stored on his computer was examined by a computer expert who found an exceptionally high number of pornographic images of children of an extremely perverse and unpleasant nature."

Mr Coombes added that the evidence showed that Hansford had sent indecent photographs of young girls, aged 16 or younger, to others using the Internet, as well as messages telling other users that he would be prepared to "trade new for new".

And he submitted a message to a bulletin board, which anyone with a computer could have access to, asking for material and guaranteeing "great pictures by return".

Another message said: "Trade? I have lots and lots. I'll send as soon as I receive."

Mr Coombes said one picture appeared to show the rape of a boy aged five or six, with other pictures showing youngsters aged from about five to 12.

He said: "He was fascinated by the difficulty of sending the stuff and had been asked to be put on mailing lists, saying he was so concerned by his own curiosity he had seen a counsellor."

In transcripts of police interviews read out in court, Hansford said he had owned his computer for two years and that he was repulsed by child pornography, but interested to see how easy it was to find. He told the police that he collected the material because it was a challenge.

He said in the transcript: "To my shame I became quite good at finding all sorts of stuff. But curiosity was the key, not perversity."

Richard Sones, defending, said that Hansford had been working as a journalist and was simply exploring the extent of what was available using the Net. He said: "Using the Internet was a hobby. It appeals to the curious and explorative sides of people's minds.

"This man has a very inquiring mind. In developing this interest of the Internet he has been pursuing a very normal and legitimate interest, but he has been utterly stupid."

"It shocked him. He is not a paedophile. His first thought was to establish the extent with which this material could be sent. But for some reason it didn't work this way."

Mr Sones, who himself admitted that some of the material was "dreadful and disgusting", said that Hansford had received unsolicited pictures from other users after entering chat rooms on the Internet.

He said: "He should have deleted this from his storage and he did this for the first few months but back log built up and he was found in possession with it.

"All those who know this man say he is a perfectly normal, respectable, hardworking and caring man. But now it appears he has not got a foreseeable future."

Judge Richard Hawkins said he had found looking at the pictures very distasteful and added: "Let me be quite clear that it is a very serious matter to distribute photographs of that nature.

"These pictures are of a wholly disgusting nature. A prison sentence is quite inevitable for offences of this kind."

Hansford was jailed for 12 months for the distribution of the material and sentenced to six months imprisonment, to be served concurrently, for the counts of possession.

He was also ordered to register with the police under Sex Offenders Act 1997 for the next 10 years. The law, which has only just come into force, requires those convicted of sex crimes to give their names and addresses so local police can keep track of them.

After the hearing, Det Sgt Richard Burkmar and Det Con Danielle Colley, from Dorset Police who led the investigation, said the sentence showed both the police and courts were prepared to take tough action.

Det Sgt Burkmar said: "I hope the sentence will act as a deterrent to anyone else thinking of using the Internet for this purpose.

Det Con Danielle Colley said: "We've put a lot of work into this and we got a good result. It's important that people realise that this is a very serious crime and that it can't be taken lightly.

"There are sure to be more cases like this across the country. It's really just the tip of the iceberg."

Case study

The behind the scenes work by detectives and computer investigators helped secure the conviction and sentencing of Jean-Paul Hansford. Here Peter Verreck, of Computer Forensics Ltd, explains how the evidence was presented.

No matter how exacting, precise and accurate the forensic analysis is, the value of the evidence will ultimately depend on the way in which it is presented in court. This was well illustrated in the Hansford case where pornographic material was presented to the court in a manner that fully showed the seriousness of the offence and resulted in a maximum sentence.

Background

Officers at Dorset Constabulary Child Protection Unit received information from the FBI in the USA that files containing child pornography had been transmitted to an e-mail address in the Bournemouth area. Subsequent enquiries revealed the address to be that of a man who worked as a disc jockey at a radio station on the Isle of Wight. A search warrant was obtained and the man was arrested following search and seizure operations carried out at both his home and workplace.

Items Seized

In addition to printed material a Pentium based computer system was seized at the suspect's home address together with a small quantity of floppy disks.

Interview and Charges

At initial interview the suspect admitted that there were graphic files on the computer containing pornographic pictures of children. He further stated that he had downloaded these from the Internet and that he had forwarded some files to other paedophiles. He was charged with possession and distribution of child pornography, to which he pleaded guilty, and released on bail.

At subsequent interview with both the police and probation service he claimed that he had no interest in children and had originally downloaded a few files in order to conduct research for a radio programme he was planning. He further stated that when he saw how unpleasant the material was he decided to cease research and cancel the planned programme. Subsequently, he claimed, because he was now known to paedophiles with whom he had made contact, whenever he switched his computer on pornographic images of children were transferred automatically to his hard disk. He said he was powerless to stop this process and that this was the reason there were so many images on his computer.

Forensic Examination

The computer system was copied and analysed using DIBS® forensic equipment. The hard disk was found to have a total data capacity of 1.0GB of which 961MB was occupied and 71MB free. The computer was operating under MSDOS Version 6.22 and Windows 3.11.

The hard disk was copied to optical cartridge, which was then write protected, prior to being automatically reconstructed using a standard forensic workstation. The reconstructed drive was initially examined and then later booted to give direct access to e-mail logs. A file listing was produced which showed that there were a total of 13,472 files. This was sorted using file extensions for common graphics file types BMP, JPG and GIF. This indicated the presence of large quantities of files of the JPG type, and smaller quantities of the GIF type, located within two main sub-directories.

When the recreated hard disk was booted the e-mail logs were simple to access and these showed the addresses to which graphic files had been sent together with the file names.

Results of the Examination

There were a total of 2,853 JPG files and 225 GIF files on the computer. The contents were examined and the vast majority were found to contain pornographic images of children of a most perverse nature.

The graphic file names found in the e-mail logs were checked against files of that name located on the hard disk and found to contain pornographic images of children. The machine dates and times at which these were transmitted were obtained.

Presentation

1. Presentation Priorities

Whilst the accused was pleading guilty to the offences he was also offering a justification for his actions: that he had no personal interest in paedophilia and had been unable to stop the automatic transfer of files to his hard disk following his research for a radio programme.

This excuse might have confused court officials who had no experience of the Internet. The priorities were therefore: to clearly illustrate the sheer volume of pornographic images contained on the machine together with the extremely perverse and unpleasant nature of the material involved; to show that there had been deliberate onward transmission of the material; to show that there was an active interest in paedophilia reflected in other material on the hard disk such as fantasy stories involving sexual acts with children.

2. Printing of Graphic Files

All the graphic files were printed out as 'thumbnails'. There were thirty of these per A4 sheet. A total of 2,797 thumbnails were printed. Graphic files not printed were either corrupted or contained no pornographic material. Then 37 representative images were selected and printed full size on A4 paper.

In order to print such a high volume of graphic images the files had first to be copied to a working optical cartridge from which they were then printed as groups. On all graphic prints the location of the file within the DOS structure on the original hard disk was indicated at the top of the print. An additional reference located the file within the structure of the working optical cartridge.

3. Criteria for Selection of Images as Child Pornography

The criteria used to consider an image as child pornography were that it should clearly depict a child or children posing or indulging in sexual acts and plausibly below the age of 16 years. Adolescents and children possibly 16 years or over were not considered as child pornography.

4. Main Report and Appendices

The main report was concise and clearly described the physical characteristics of the computer, the forensic techniques used, and the results of the analysis. This was supported by eight appendices, five of which contained the 37 full size prints which were the specimen charges for the offence of possession of child pornography. Each of these was prefaced by a written description of the material which followed, including estimates of the apparent ages of the children involved. For example "Appendix 5 - A series of eight colour images of the sexual assault and oral rape of a young female child of apparent age eight or nine years".

Appendix 6, which formed the bulk of the report, contained the 'thumbnail' prints. The remaining appendices contained e-mail files and logs showing that distribution had taken place, and examples of text files containing obscene fantasy stories involving the sexual abuse of children.

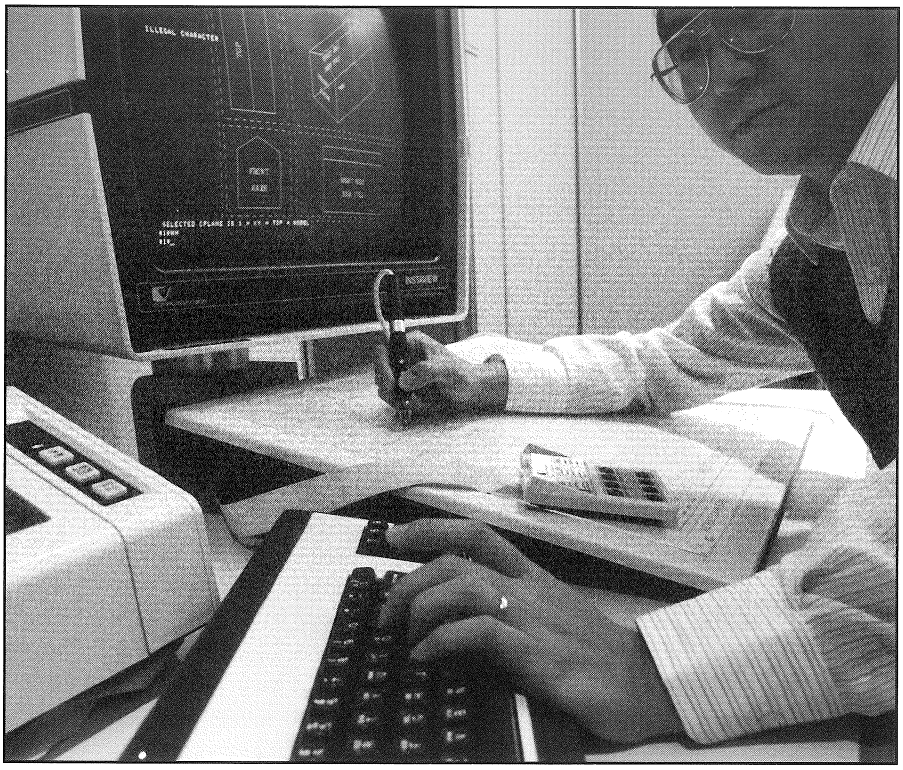
5. Distribution of the Report

Due to the extreme nature of the material only two full copies of the report were made, one for the prosecution and one for the judge. The defence received a copy without graphic material and viewed the full prosecution copy under supervision. At the conclusion of the case the judge ordered that his copy should be destroyed.

Conclusion

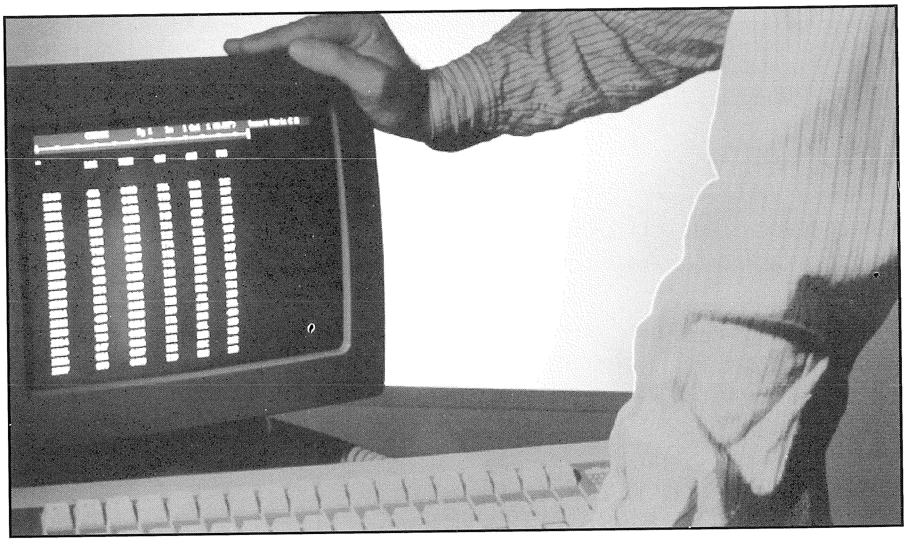
The court was made fully aware that the computer hard disk contained an exceptionally high volume of graphic material of an extremely perverse nature, the vast majority of it involving children. It was emphasised that the volume was such that collection would have taken a long period of time at considerable expense, and that this finding was consistent with what might be expected for a computer owner with a long-term, serious, escalating, sexual interest in children. It was further shown that the material has been redistributed on a regular basis by the computer owner to both other individuals and to paedophile groups.

The court imposed the maximum six month custodial sentence for possession of child pornography together with one year for distribution. The offender was also subject to the Sex Offenders Act and required to register for 10 years following release.



Book review

Nabarro Nathanson: The Laws of the Internet
By Clive Gringras LLB
Butterworths,
London WC2A 1EL
Price £85



If we are to believe everything we read in the press, the Internet is like the Wild West - a brave new adventure but a place where laws do not exist and bandits roam freely.

The suggestion is that current laws, both national and international, cannot cope with the breakdown of barriers, the lack of geographical or political borders and the technical complexity of policing legislation.

But while the Internet certainly is vastly different from many systems of communication that society is familiar with, this does not mean that it cannot be approached and discussed in a logical way.

Certainly lawmakers, enforcement agencies and lawyers were initially taken aback by the sheer scale and inherent difficulties, but this is gradually being replaced by a more considered examination of just what can and cannot be done.

Governments across the world are now tackling the subject, and already there have been many successful investigations and prosecutions of those who flout the rules.

The Laws of the Internet tries to debunk the myths and black art surrounding Net law and put the problems into perspective.

It has been written mainly for the legal community and aims to present a practical view of current laws affecting the Internet, either directly or indirectly.

Gringras has based the book around British laws and he covers the major areas which apply, such as copyright, jurisdiction, contract, crime, data protection, financial laws, taxation and banking. Tort is also discussed, including special variants of torts such as negligently allowing a virus to spread and new ways of defaming people.

He gives an overview of the law and then goes on to show how it could be applied by using real-life cases and comparing them to situations that could happen online. Because Net law is a relatively young subject, Gringras has used his imagination to create the problems but answer them according to real legislation.

This method of comparison helps the reader to understand both the theory and the practical implications while avoiding the huge pitfall of getting too bogged down in pure law.

As Gringras says in the book: "There is no single law that does or should apply to the Internet. The book is concerned only with the application of the current body of law to this new communications medium.

"Often these answers are to questions not yet asked of English courts. For the moment, therefore, the readers is the sole judge of their cogency."

Gringras is well suited to discuss the application of laws on the Net - he is an experienced programmer and qualified lawyer and has advised New Scotland Yard on computer crime as well as writing for UK technology and law publications.

As with any area of the Internet and the computer world, the speed of technical change that happens is staggering and can make any printed reference work virtually useless within months or years.

While the Net is evolving every day, Gringras has imposed a degree of future proofing of his book by basing it squarely on the laws involved so that the principles and procedures discussed will stand even when technology has leapt ahead.

The book does not try to be a stand alone reference work, and the author acknowledges it works best in conjunction with other legal and technical books. However, the writing is exceedingly clear and concise and is free of the jargon which can easily afflict a book of this type. The reader is given a thorough grounding and understanding of the most important areas, although a book of this type cannot go into absolute minute detail.

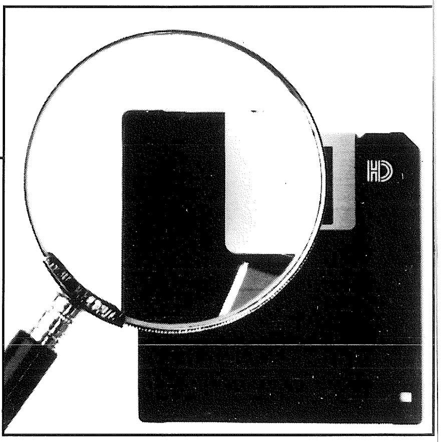
All topics are fully referenced and comprehensive tables of statutes and cases are included, along with the relevant page in the book. And for the many who find the whole subject of computers and Internet confusing, there is a full glossary covering all the major terms and systems.

Overall the book is an interesting and useful read that reflects the current position of the law in the UK regarding the Net as well as predicting what the future holds. Its intelligent and practical style means that it can be used by anyone involved in the field, including lawyers, students, police officers and investigators. The chances are that if you have a question regarding some aspect of Internet law, it will be addressed in the work or at least point the way to go for further research.

The one caveat is that the book is very much UK-oriented, which means the laws in other countries may well not apply in the same way.

However, it still gives an indication of the current position on what can and cannot be done on the Internet, and what provisions are likely to be made in the future. Recommended.

Forensic Q&A



Q I have been called to the scene of a crime where the computer is still turned on. How can I correctly examine the contents of the memory?

A Before answering the question let us first emphasize yet again that whenever a computer is found turned on at the scene of a crime it is most important that:

1. The exact state of all the computer equipment is recorded prior to any action being taken. This may include written records, photographs, sketches and videos

2. A record is kept of all actions performed whilst examining the system. A small tape recorder is very practical for this purpose. A running commentary can be maintained of all actions i.e. 'I am going to press the enter key on the keyboard. I am now pressing the key. I pressed the key once and then removed my hand from the keyboard. The display on the monitor has now changed to ....' etc.

3. The suspect is never allowed to touch the computer. If the computer is running a version of Windows and multiple programs are in use then the Alt-Tab key will display the contents of suspended screens that are currently being held in memory.

If a printer is attached these can be output using the Print Screen key. Once this information is recorded Windows can be unloaded and the DOS program MEM run from a forensically sound floppy disk (remember that the version of MEM that you run should match the version of DOS with which the machine was booted).

MEM will display information about allocated memory areas, free memory areas, and programs that are currently loaded into memory. Using the switch, / classify, a more detailed listing will be produced of all memory areas and all programs that are running. For example in a recent murder inquiry a computer, found turned on at the scene of the crime, was running Windows 3.11 with a screen saver active. Using the Enter key and Alt-Tab the screen saver was disabled and the work in progress on the word processor was displayed. This was a part-written letter which was printed out. Windows was then unloaded from memory. The MEM command showed that no other programs except known drivers were running and the machine was then shut down prior to full copying.

Q I have been told that I should not boot a computer for forensic purposes using DOS 6.22. Why is this and what should I use?

A The problem with all versions of DOS from 6.00 onwards is that Microsoft introduced drive compression into the operating system. One result of this is that when booting from a floppy the file COMMAND.COM looks at the hard drive to see if it is compressed. If it finds that it is then it activates the file DRVSPACE.BIN which prepares the compressed file on the hard disk for unpacking. In the process a log file is written to the hard disk. Obviously when booting an unknown computer it is impossible to tell if it has a compressed drive. If it does then the evidential integrity of the machine will be compromised when the log file is written to the hard disk.

For forensic purposes booting should only be performed with a version of DOS earlier than 5 which did not have compression. Furthermore, a forensically sound boot disk should be on a 720KB floppy so that it will be recognised by older machines that did not read 1.4MB disks.

Incidentally, you cannot cure the problem by deleting the DRVSPACE.BIN file from the floppy disk. This may cause the boot sequence to load and execute the DRVSPACE.BIN on the hard disk.

Q I am examining a hard disk for evidence of forged documents and suspect that I may find the evidence in temporary files. Is there a general location for these files and are they systematically deleted by the computer?

A There is no definitive answer. It depends on the programs that have created the temporary files and the way in which the computer has been set up. Most programs will allow you to specify the location of temporary files although most users don't do this. Programs which create temporary files should clear up by deleting the files after use. If you need to find temporary files the best approach is to create a list of all the files on the computer, including deleted, and then sort them by file extension using a suitable program. This is always a very powerful technique for isolating possible relevant information and focusing the investigation.

Q I often used file manager in Windows 3.11 to get an overall impression of the files on a copied suspect PC. Quite recently I found that I could only display files with a BMP extension. When I looked in DOS I could see all the files. What is causing the problem?

A The most likely cause is due to a bug in file manager. It happens, very occasionally, after a search has been performed, using FIND, for files with a particular extension. The effect of the bug is to reset the view file type parameters. I suspect that you had performed a search for files with the BMP extension and it was after this that the problem occurred. To correct it select VIEW from the menu bar and then select BY FILE TYPE from the drop-down box. You will find that the NAME box is set to *.BMP. Reset it to *.*. You will also find that if you had SHOW HIDDEN/SYSTEM FILES set it will now be un-set. Re-set this as well (when using file manager this should always be set).

If you have any tips or advice you would like to share, please contact the Journal. E-mail questions to ijfc@pavilion.co.uk

Although every effort is made to ensure the accuracy of these answers, they are presented for general information and may not apply in rare specific cases. Readers are advised to seek confirmation from an independent specialist in forensic computing when dealing with evidentially valuable material.

Notice Board

We will be pleased to receive contributions to this page. Please mark all correspondence 'Notice Board'. We reserve the right to edit if required.

Events

Compsec 97
The 14th world conference on Computer Security, Audit & Control

-7 November, QEII Conference Centre, London

A 'new larger COMPSEC' offers the opportunity to visit companies producing the latest hardware, software and techniques with advice from some of the best names in IT security.

The Sixth Annual Directors' Briefing on 6 November will provide a complete non-technical overview of computer security and its implications at board level.

Dr Bill Hancock (author of 24 books on computer networking and security and experienced computer and network designer/engineer) will present an extra day of pre-conference seminars.

The Main Four Stream conference will include over 60 sessions of computer security advice.
Contact: COMPSEC Int. 97
Tel: +44(0)1865 843643
Fax: +44(0)1865 843958
E-mail: a.richardson@elsevier.co.uk

The Third Annual Superstrategies Conference

11-13 November (Optional Workshops 10 November), Grosvenor Thistle, London

Sessions cover issues and topics with the most impact on audit departments today including Internal Audit's Role in an Organisational Fraud Strategy: The organisational fraud team, Setting and establishing organisational fraud policies, Ongoing fraud monitoring, Strategies for policy improvement; and Improving the Control Environment: Understanding Individual Behaviour Within the Organisation.
Contact: MIS Training Institute
Tel: +44(0)171 779 8944
Fax: +44(0)171 779 8293

Information Management '97
11-12 November, London

The conference will expound the latest strategic thinking in Information Management, explain the impact of the new generation of enabling technologies and present revealing case studies from leading-edge enterprises.

Speakers include Philip Webb, Information Systems Director, DERA and Bill Mayon-White of the LSE and Convenor of the IDMA.
Contact: Elan Conferences Ltd
Tel: +44(0)1225 330312
Fax: +44(0)1225 330305
E-mail: elan@cix.compulink.co.uk

Milipol Paris 1997

24-28 November
Le Bourget Exhibition Centre

Contact: IMEXPO
Tel: +33 01 46 27 82 00
Fax: +33 01 46 27 91 63

International Internal Auditing

8-12 December, London

Specifically designed by City University Business School, this conference brings together senior internal auditors from around the world providing delegates with an essential update on state of the art developments. There will also be the opportunity for participative discussions within and between sessions.
Contact: Prof. Georges Selim, City University Business School
Tel: +44(0)171 477 8710
Fax: +44(0)171 477 8882

White Collar Crime Course

2-4 December 1997 and
24-26 February 1998, London

This course has been planned to provide a foundation for those whose duties include the responsibility for investigating fraud and breaches of financial regulations.
Contact: International Conference Group Ltd.
Tel: +44(0)181 743 8787
Fax: +44(0)181 740 1717
E-mail: icg@inconference.co.uk

International Conference for Criminal Intelligence Analysts

17-19 March 1998, Manchester, UK

The aim of the conference will be to provide a forum for the discussion of the emerging threats from serious criminal activity over the next decade and the analytical techniques for combating them. The focus will be on the strategic and operational analysis of criminal activity, particularly in the high-tech sectors, and how a multi-disciplinary approach can best be developed by analysts worldwide.

To be hosted by the UK's National Criminal Intelligence Service and the Henry Fielding Centre for Police Studies and Crime Risk Management (University of Manchester);sponsored by Europol Drugs Unit, Swedish NCIS and i2 Limited, Cambridge, UK.
Early booking is advised.
Contact: Paula Whitehead, Henry Fielding Centre, Manchester University
Tel: +44(0)161 275 4769
Fax: +44(0)161 275 6861

Net Gambling law symposium

11 - 13 November, JW Marriott Hotel, Washington DC.

The conference is the first of its type and will cover the legal and regulatory implications of new technologies and gambling.
The seminar will include sessions on state and federal law, off-shore structure, international law, creating the virtual casino, software development, enabling technologies, contracts and case studies and industry self-regulation.
Promoters of the conference say that there are already a huge number of betting web sites and that by the year 2000 Internet gambling will be a $10 billion industry.
Contact Mary Ann Liebert Inc
Tel: +1 914 834 3100 ext 652

International Journal of
FORENSIC COMPUTING™

Published by
Computer Forensic Services Ltd