ISSN. 1363-6650

NOVEMBER 1997
Issue 11

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

Computers and telecommunications technology have cut the size of our planet to ribbons.

Mail and data can be sent instantly across the globe at the press of a button and users in different continents can chat to each other for the cost of a local phone call.

And the phenomenon of the Internet allows an incredible level of contact and access to information unheard of until only a few years ago, creating the largest database and library anywhere.

The computer community is truly a global village, making a mockery of physical distances and individual borders in any country.

Pretty obvious and prosaic? Maybe, but the message is still to get through to a lot of investigators and police officers working in the field of forensic computing across the world.

Too many still have a "my back yard" outlook, and will only look as far as the crimes in their immediate jurisdiction and territory. This is an outdated concept in policing, with the huge risk that many criminals will go uncaught or unchallenged.

What is needed is greater co-operation between everyone in law enforcement groups, from those working on computer investigations down to the officers on the beat.

If a cyber crime is spotted by one police department but the suspect is from a different geographical area, then this vital information has to be passed on to the relevant authorities.

This is already happening to great effect by the more switched on groups. For instance, paedophile Jean Paul Hansford was investigated, prosecuted and jailed in the UK after a tip off from the FBI in the US. The FBI contacte Dorset Police after monitoring files con taining child pornography that were sen to an e-mail address in the UK.

Without the communication and co operation, the case might never hav come to light. But there are probabl hundreds of thousands of paedophile who remain unchallenged just because in formation has not been shared.

If the criminals can make use of th technology to communicate with eac other, why can't the good guys who ar trying to catch them?

And similarly, police across the worl need to keep up with the latest develop ments in computer crime, investigatio and law worldwide, even if they are no faced with those specific problems i their own territory at the current time.

The global computer communit moves fast, and problems and solution in one country will quickly move to oth ers within years, months or even days.

For instance, much of the news car ried in the Journal looks at events in th US, where computer crime is now a everyday occurrence and techniques an legislation are being hustled in to try t deal with it.

As with many other facets, from ham burgers to handguns, the US leads in th levels of computer misuse and othe countries are sure to follow this path.

Does this matter to the investigato as far afield as the UK, Finland, Asia o Australia? It surely does, because law enforcement groups in those countries have the chance to examine the real is sues, both technical and academic, so they can be ready when the time comes.

Hiding your head in the sand is fine for an ostrich, but it could be disastrous for forensic computing.

News

Action over alleged Net pirates

A lawsuit has been filed against two people in the US accusing them of putting copyrighted software on the Internet for others to download.

The Software Publishers Association, a copyright protection watchdog, is taking the legal action on behalf of seven of its member companies., including Adobe, Claris, Corel and Intuit.

Before filing the suit, the SPA subpoenaed two Internet service provider firms for the names of the site operators offering the material through two Web sites.

Both sites provided bootleg serial numbers for installing pirate software and software piracy tools designed to get around technical protection measures.

The addresses of the sites, which the ISP have now removed or blocked for general public access, were www.velocity.net/~overlord and chisel.toolcity.net/~overlord.

Filed in the US District Court for the Western District of Pennsylvania, the suit came after an exhaustive seven month investigation tracking each site and monitoring the alleged infringing material on each site.

More than 53,000 people, visited the sites during that time period, and all of them had access to the material being offered. The sites provided an extensive list of serial numbers for about 4,500 software products, some of which sell for thousands of dollars. When printed out in hard copy format, the list runs to 78 single-spaced pages of serial numbers.

Director of North America anti-piracy Peter Beruk said: "These Internet sites, and thousands of others, have become a place to fence and acquire pirate software.

"Bootleg serial numbers enable people to use pirated software downloaded from other sites, and software piracy tools let them make unauthorised copies.

"This is only the tip of the iceberg. This lawsuit is the first of its kind alleging this type of infringement, a type of piracy which has become far too common on the Internet.

"In fact, a recent search for illegal software on the Net revealed nearly 17,000 different sites offering infringing material."

Net used by racists

A report by the Anti-Defamation League says that the Internet is being increasingly used by racists, anti-Semites, anti-government extremists and others who spread their hate.

ADL members fear that hate is "polluting the Internet" and that offenders can now "spew their hate easily, cheaply and often deceptively, reaching numbers they could only have dreamed about before the telecommunications revolution."

In the ADL report, called "High Tech Hate: Extremist Use of the Internet", officials say groups such as the Ku Klux Klan go online to recruit and spread propaganda.

ADL's website at www.adl.org has information on identifying hate groups and fighting them.

Anti-spam war

Internet service provider America Online is continuing its campaign against unsolicited e-mail by taking alleged culprits to court.

AOL filed a suit in Virginia, US, against Vernon Hale and Prime Data Worldnet Systems Inc seeking to block what it described as "get rich fast" spam mailings which it said have resulted in millions of unsolicited e-mails being sent to its subscribers.

And AOL said Hale and Prime Data Worldnet Systems have used unsolicited mass e-mail to sell two programs, Floodgate and Stealth, to other would be spammers.

Floodgate can gather e-mail addresses from various sources on the Internet, while Stealth can provide mass mailings with false return addresses in order to evade filters and other measures designed to block spamming.

Associate general counsel for AOL, Randall Boe, said he wants to know how many spam letters have been sent out and how many copies of the software have been sold on to others.

He said that the aim of the suit is to "try to find out exactly how many pieces of mail he has sent to us and exactly how much he has damaged our service, and ultimately to get an order barring him from continuing to send unsolicited mail through the AOL service."

A spokesman for AOL said: "Spam is an annoying intrusion for users of the Internet and the result is aggravation and slower e-mail service.

"The days of no accountability for spammers are over. We will make sure that spammers are held accountable to the law."

The latest suit comes after AOL announced it was to sue Las Vegas-based Over the Air Equipment Inc from sending bulk e-mails to its members. And in February, a federal court in Philadelphia ruled on an AOL-filed suit and ordered CyberPromotions Inc to stop using fictitious and unregistered domain addresses to send unsolicited e-mail to AOL subscribers.

Man jailed for Internet abuse

A man dubbed the "Internet Romeo" was sentenced to more than five years in prison in the US for using an online chat room to solicit sex with a teenager.

Keir Fiore, 21, from Manchester, New Hampshire, pleaded guilty to two counts of interstate transportation of a minor for illegal sex after using the Net to talk to a 13-year-old girl in Salem.

Prosecutors said Fiore flirted with the teenager and then convinced her to run away with him. The pair were eventually found by police after a national search.

Fiore read a statement out to the court apologising to the teenager and her family. He said: "The Internet is dangerous for young children who use it without parental supervision."

He was sentenced by US District Judge Joseph DiClerico to five years and three months in jail.

Prostitutes online

Police in Minnesota, US, have used the Internet to publish pictures of alleged female prostitutes and those who are accused of being their customers.

Officers in the St Paul Police Department said the 12 colour photographs were of people arrested for engaging in pros-

titution within the last 18 months.

The site carries the disclaimer that "all persons are considered innocent until proven guilty in a court of law."

Police in the town now carry digital cameras and will file pictures along with their written arrest reports. The web page will be updated weekly and includes the names, hometowns and ages of the women, and the same information for the men as well as their car make and model, registration plate and the road where they were arrested.

A spokesman for the police department said: "The photos and descriptions in this section will help St Paul residents identify and alert police to this criminal activity.

"Residents are tired of prostitutes plying their trade on their sidewalks. They do not want their girls and women treated with disrespect by customers coming into their neighbourhoods.

"And they do not want their children to view acts of prostitution enacted in public places at every hour of the day and night."

The Internet site is at http://www.stpaul.gov/police

Pager messages intercepted

A news agency in the US has admitted breaking the law by intercepting pager messages from the police and selling tips on to newspapers and television stations.

Breaking News Network has pleaded guilty, along with its owners and general manager, of illegally intercepting messages from public agencies, including the New York Police Department.

BNN, based in Fort Lee, New Jersey, pleaded guilty to one count of illegally manufacturing and possessing software and cloned pagers programmed to intercept police and fire department pager messages.

Owners of BNN, Steve and Robert Gessman, of Cliffside Park, New Jersey, and general manager Vinnie Martin, of North Bergen, New Jersey, also pleaded guilty to the same charges. BNN faces a maximum fine of $500,000, while the three individuals face a maximum penalty of one year in prison and a $10,000 fine each.

US Attorney for the Southern District of New York, Mary Jo White, said the arrests and convictions against BNN mark the first-ever prosecutions and convictions of unlawful interceptions of messages sent to pagers.

She said: "These arrests should serve as a wake-up call to all who would be tempted to snoop on the electronic communications of others."

Charges still are pending against a fourth individual, Jeffrey R. Moss, of Manhattan, a former "dispatcher" for BNN, for the unlawful interception of paged messages sent to, among others, the NYPD, NYFD, the New York City Office of Emergency Management, Emergency Medical Services, a New York City Commissioner, and a New York City District Attorney's Office.

Moss also was charged with the unlawful possession of a computer software package called "Message Tracker" that allowed him to monitor messages sent to those pagers and others.

The arrests grew out of a NYPD investigation called Operation Pagergate and after first uncovering the alleged scheme, the NYPD teamed up with the FBI's Electronic Crimes Task Force.

White said that in early 1997, Martin gave a confidential informant, who worked as a BNN "dispatcher", a cloned pager that was programmed to illegally receive intercepted pager messages. Gessman then instructed the informant to use the cloned pager in connection with his duties for BNN.

According to White, the informant gave the cloned pager to a Secret Service agent, and an analysis revealed that it was a cloned NYPD pager also programmed to intercept messages being sent to an individual in the Office of New York City Mayor Rudolph Giuliani.

Along with being a "wake up" call to criminals, White also said the case was a message to the public, as well as the business and law enforcement communities of America.

She said: "If you are using a paging system, your communications may not be secure. No governmental agency or business is immune from this illegal monitoring."

Hong Kong decency code

The Hong Kong government and Internet service providers are issuing a code of practice in a bid to stop indecent and obscene material online.

Officials hope the measures will prevent users placing and sending illegal pictures and text, including pornography.

The Hong Kong Internet Service Providers Association, which has 40 members, said it would block web sites which were found to contain obscene material once it received a complaint.

A spokesman for the society said: "We have consulted all our members in drawing up the code of practice and have obtained their full support in its implementation.

"All our members agree that they have an important social responsibility to fulfil."

Swiss man arrested in porn sweep

A computer assistant at Basle University in Switzerland has been arrested and charged with possession of Internet pornography.

The 31-year-old was targeted after a tip-off led police to examine the university Web site server, which was shut down while officials checked it. When police raided the man's home they found further pornographic images on his own PC.

Possession of child pornography is not an offence under Swiss law, but the man could be charged with transmitting the online material and if found guilty sentenced to up to three years in prison.

Law to handle cyber signatures

Legislation to clarify the use of so-called digital signatures could be introduced across the US to boost Internet business.

Senator Bob Bennet told a hearing of the Senate Banking Committee's financial services subcommittee that federal action was needed to prevent individual states introducing their own, possibly

nconsistent, laws which might stifle nline commerce.

He said: "Internet transactions do not espect state boundaries and it may be difficult for parties to determine which state law governs a particular transaction."

Digital signatures, which include identifying codes attached to electronic documents, are used to verify and authenticate e-mail and contracts over the Net.

About 14 states already have laws governing electronic agreements, but some financial industry leaders fear that contradictory standards could badly hinder trade.

Alfred Pollard, senior director of the Bankers Roundtable, said: "State laws that conflict with one another as enacted or that may conflict under regulatory or judicial interpretation, run counter to the critical need for certainty in the authentication process."

Senator Bennet has not released specific details of his proposal but said the bill would be introduced early next year.

Internet filtering and content meeting

Delegates to a conference in the US heard about the latest developments in the fight to curb the worst excesses of the Net.

The meeting, sponsored by Digital Equipment and called Balancing the Scales, was held in Washington DC and focused on the rights, responsibilities and technologies at the heart of the debate.

It also examined the next generation of solutions to protect children and increase the scope of business carried out on the Web.

Director of business development for Digital's AltaVista search engine Abe Hirsch said: "Our goal is to look at solutions for Internet content filtering that go beyond simply protecting children from objectionable, sexual material.

"A new approach is needed to do more than just protect children from inappropriate material. Solutions must also assist in greater productivity and allow many diverse communities on the Internet to view the Web in accordance to their interests or unique points of view."

Web users tricked by trade marks

Website managers are breaking the law to lure Net users to their pages, warns the UK Institute of Trade Mark Agents.

According to the IoTMA, there are many thousands of breaches of trade marks hidden in the subscripts of websites. These "invisible" words cannot normally be seen but act as identifying tags when a user searches for specific words or phrases.

Trade mark experts at the Institute say many businesses are using their competitors' names buried in their own websites to increase the number of page hits and steal trade.

Ian Buchan, of the Institute, said: "Be warned. In the US this activity is now the subject of litigation under trade mark law. Companies are being sued for trademark infringement and unfair competition.

"What happens in business litigation in the US today invariably happens here tomorrow."

The Institute advise all businesses to carefully police the use of their trade mark names on the web, and warns that those abusing the system could face being sued and paying sizeable damages.

Mr Buchan added: "As more organisations, particularly smaller businesses, begin to trade on the Internet, this level of protection will become more important than ever.

"Don't let your competitors steal a march on you, and don't let them capitalise on your name and investment."

Thieves grab millions in software

Raiders broke into printers working for Microsoft in the UK and stole CD-ROMs and authenticity certificates worth up to £30 million.

No actual finished product was stolen, but the thieves got away with more than 100,000 CD-ROM discs plus documentation which could be used to create pirated software packages.

A gang of four masked men, one armed, attacked and overpowered two security guards at Thompson Litho, in East Kilbride in Scotland, a company that is authorised to produce official Microsoft products.

The gang escaped with 200,000 authenticity certificates and copies of MS-Office, Encarta and other applications, all of which could be used, company officials claim, to create up to £30 million worth of illegal software.

Net censoring blasted

New legislation in the US aimed at banning online material deemed "harmful to minors" would run roughshod over the law, according to the American Civil Liberties Union.

The ACLU fear that the law would run counter to a landmark US Supreme Court decision affirming free speech on the Internet.

The legislation, introduced by Senator Dan Coats, an original sponsor of the Communications Decency Act struck down by the Supreme Court in June, would amend section 223 of the Communications Act of 1934.

It aims to "establish a prohibition on commercial distribution on the World Wide Web of material that is harmful to minors, and for other purposes".

The bill, referred to the Senate Committee on Commerce, Science, and Transportation, states that "whoever in interstate or foreign commerce in or through the World Wide Web is engaged in the business of the commercial distribution of material that is harmful to minors shall restrict access to such material by persons under 17 years of age."

Offenders would face fines up to $50,000, and up to six months in jail.

The bill also requires Web sites to use a verified credit card, debit account, adult access code, or adult personal identification number to determine if a person accessing the site is over 17.

ACLU national staff attorney Ann Beeson said: "By claiming that the bill address only Web sites involved in commercial distribution, Senator Coats says he is 'hunting with a rifle,' but in fact has lobbed another virtual grenade attack into the heart of the Internet."

Unlike the CDA, Coats' bill only applies to Web sites, and not to chat rooms, e-mail or news groups.

Beeson added that under Coats' bill,

any business "merely displaying material without first requiring a credit card or other proof of age could be found liable under the statute, even if no actual sale is involved.

She added that there also are "serious constitutional problems" as well, with the bill's definition of "harmful to minors".

Arrests in clone phone scams

A US man has been arrested and charged with operating a clone phone scheme.

Juan Pena, from Lynn, Massachusetts, who was previously arrested on a criminal complaint, was indicted by a federal grand jury and charged with violating federal telecommunications fraud law.

According to the indictment, Pena not only trafficked in clone phones, but possessed sophisticated computer equipment in order to complete the cloning process.

A cloned phone refers to one in which the numbers assigned to a legitimate cellular telephone subscriber are illegally obtained by the cloner, and then programmed, usually using special computer software, into another cellular phone.

That phone is then sold by the cloner to a third party and when the purchaser of the cloned phone makes calls, those calls are then billed to the legitimate cellular telephone subscriber's account.

According to US Attorney Donald Stern, fraud costs cellular carriers more than $650 million a year nationwide.

Stern said Pena was also charged with possessing a scanning receiver, computer hardware and software and a "copy cat" box to illegally obtain telecommunication services.

If convicted, Pena faces maximum penalties of up to 15 years imprisonment and a fine of up to $250,000. The case was investigated by the US Secret Service and is being prosecuted by Assistant US Attorney Nadine Pellegrini of Stern's Major Crimes Unit.

- The St. Paul Police Department in Minnesota arrested 28 people using cloned cellular phones to conduct illegal drug sales in a two-day sting operation.

The dragnet culminated two months of police investigation together with AirTouch Cellular.

LeAnn Talbot, vice president and area general manager for AirTouch Cellular in the Midwest region, said the sting centred around a simulated cellular store in St. Paul.

AirTouch provided signs, training, equipment and cellular airtime needed to run the storefront, she said, while undercover officers sold cloned phones from the location, and in the process gathered evidence which led to the arrests.

A new bill, the Wireless Telephone Protection Act passed by the US Senate, would amend the federal criminal code to crack down on those who try similar phone scams.

While the legislation includes exceptions for legitimate investigative use by law enforcement and the telecommunications industry, it provides increased penalties for a second or recurrent offence for fraudulent activities involving counterfeit communications access devices.

Return of the spam

When mass commercial e-mailer Cyber Promotions was forced off the Internet last month, president Sanford Wallace vowed to return.

Now it looks like the self-styled "spam king" is about to make good on his promise with the launch of his own network, dedicated to sending unsolicited commercial e-mail, known as spam.

In a press release apparently from partner Walt Rines, via a Hotmail e-mail account, the two wrote, "Sanford Wallace, Walt Rines and an undisclosed third party have formed Global Technology Marketing, Inc.

The new corporation will offer direct, high speed T-1 and T3 Internet connections to companies that engage in mass commercial e-mail.

"Currently, there are no other backbone providers that allow customers to send spam," continued the release.

Wallace lost his Internet connection after a court case that saw his service provider, AGIS, battle for the ability to disconnect his company. AGIS, which had been happily supplying his Internet connection for some time, sought to disconnect Cyber Promotions after attacks on the spam network brought down machines at AGIS.

After losing the court case, Wallace said: "The anti-spammers have not won this war, they have just made it more difficult for themselves as we will now send mail from different sources."

In the press release, Wallace said: "We are very excited about this new project. For the first time ever, Internet marketers will be encouraged to engage in direct advertising, a practice which is already accepted in the postal world."

Walt Rines said: "Finally, bulk e-mailers will have an opportunity to legitimise this new industry. We are going to prove that this explosive new market can be self-regulated."

Attack on Thailand software piracy

The Business Software Alliance is aiming to cut software piracy in Thailand by stepping up its campaign of education and legal action.

According to BSA Spokesman Huey Tan, the software infringement rate in the Asian marketplace in 1996 was approximately 80 per cent with Thailand sporting one of the highest rates, costing around US $137 million.

The BSA hopes to reduce the software piracy rate to 60 percent within the next three to five years by working closely with the Department of Intellectual Property and universities to conduct seminars throughout the country.

Recently the BSA, in co-operation with the Economic Crime Investigation Division and representatives of the DIP, raided the offices of Asian Marine Services Pcl in Samutprakarn for copyright infringement and found up to 47 unlicensed copies of software.

Baker and McKenzie Attorneys at Law representative Dhiraphol Suwanprateep said currently there are around 20 to 30 software infringement cases under court consideration, and that on December 1, the Intellectual Property court would be officially established.

Any case can be transferred from the existing court to the IP court, depending on both the victim and the accused.

Call for cybercop network in US

New York Attorney General Dennis Vacco has called on police across the US to co-operate in the fight against online paedophiles.

He spoke out at a training seminar of law enforcement personnel from more than two dozen states in an effort to forge an alliance and share resources in the battle against child porn.

Vacco, who recently was appointed chairman of the subcommittee on Internet Child Pornography of the National Association of Attorneys General, said he is "vigorously addressing" the flood of child pornography on the Internet by calling on law enforcement agencies from across the nation to join him against "this vile form of child exploitation."

He said: "Innocent children are being victimised and exploited in order to feed the appetite of these creeps who want to look at computer images of children being raped and abused.

"I am not going to stand for it. We are going to continue to lock up the purveyors of child pornography and hold them accountable for their actions."

Vacco is behind a dragnet to investigate and prosecute those who abuse the Internet by using it to download illegal material or lure children and teenagers into illegal activity.

During the seminar, Vacco urged the formation of a "new partnership of cyber cops ready and capable of tackling the growing menace of vile child pornography on the Internet."

He added: "Chat rooms in cyberspace are literally packed with perverts who are all too willing to transmit illegal kiddie porn into your home and mine with just a click of the mouse.

"To combat this victimisation of innocent children, we need to strengthen our efforts by joining forces from Maine to California. By building a new partnership of computer-savvy cyber cops, we can corner these cowards in their own and thus protect the families of America."

Vacco said evidence gleaned from a number of child porn investigations, including one involving a Staten Island man arraigned on child molestation charges, has demonstrated a connection between child porn and the sexual abuse of innocent youngsters.

He said: "Making child pornography so accessible to a paedophile is akin to throwing gasoline on a fire. It fuels the urge to hunt for victims and abuse them."

Vacco noted his office has been working with Internet service providers, including America Online, to generate information about those computer users who have been transmitting illegal child porn over the Internet.

"We have more cases in the pipeline, and we know we could do so much more with adequate resources," Vacco said. "That is why we need to assist one another and band together and share our most successful techniques and investigative methods. The price of inaction is unacceptable, because the victims are defenceless children."

He said that the investigation is expected to continue using new funding provided by the Legislature for creation of the Attorney General's Internet and Computer Unit.

- The latest success of Operation Ripcord has been the arrest of a 32-year-old man from Richmond Springs, New York, who was charged with crimes stemming from the illicit Internet transmission of child pornography.

According to Vacco, the suspect Edward Domion was charged with promoting the obscene sexual performance of a child, a Class D Felony punishable by up to seven years in prison.

Vacco said investigators found an assortment of images depicting young children being sexually exploited.

So far the ongoing joint sting operation has uncovered child porn traffickers throughout the US, and as far away as Germany, Switzerland, and the UK.

And the sweeping New York-based probe, alternately dubbed Operation Rip Cord by Attorney General Vacco's investigators, and Tholian Web by the US Customs Service, has so far resulted in over 120 prosecution referrals, and at least 32 convictions across the US, with 13 prosecutions in New York State.

Investigators have amassed more than 200,000 child porn images, and seized more than $137,000 in home computer equipment.

Refunds for fraud victims

The Federal Trade Commission in the US has promised that people who fell victim to a high-tech Internet scam will get their money back.

Users who found they had run up huge phone bills on calls after their modems were automatically switched to expensive international numbers will get refunds totalling more than $2.74 million.

About 38,000 Web surfers were lured into visiting Web sites and downloading special viewer software in order to access sexually explicit pictures.

But the software automatically disconnected users from their local Internet providers and then dialled and reconnected using long-distance numbers assigned to Moldova in the former USSR.

The FTC said that because the modems remained connected when the users left the Web sites or left the Net entirely, many of them got phone bills totalling hundreds or thousands of dollars.

And investigations showed that the calls never actually connected to Moldova but terminated in Canada, yet consumers were billed for the Moldovan-priced call.

Now the FTC has reached settlements with a number of firms and individuals charged by the agency with involvement in the scam.

This will prohibit the defendants from similar behaviour in the future as well as stop them from distributing the viewer software, called "david.exe".

Saudi censors Net

Saudi Arabia is to get a sanitised version of the Internet to make sure its citizens do not have access to offending material.

The country will introduce its own Net within six months, but the content will be strictly controlled in accordance with Islamic law.

Head of the King Abdel-Aziz City for Science and Technology Dr Saleh al-Athel said that study had been completed on how to prevent "objectionable material that goes against the country's religious and moral values".

Product News

Anti-fraud technology

A UK firm has developed an alarm system designed to combat the growing problem of dial-through fraud on telephone systems.

Foundation Data Systems, based in Christchurch, Dorset, said its Tracker system combats dial-through fraud, also known as toll fraud, which occurs when a company's telephone system is used by outsiders to make free telephone calls at the company's expense.

John Owen, a spokesperson for the company, said the activity has been prevalent in the US and Canada for some years and is fast becoming a major problem in the rest of the world. According to FDS, its system can monitor an unlimited number of telephone switches, 24 hours a day 365 days a year, and produce alarms back to monitoring stations.

The company claims that each site can be individually configured to report any unusual telephone activity both during and outside of normal working hours.

With the risk of losing thousands of pounds to hackers, the FDS says that no company can afford to be without the Tracker system.

It claims that the current growth of fraud is being assisted by the popularity of voice mail systems, the provision of Direct Inward System Access numbers and the use of private automatic branch exchange maintenance modems.

Hackers steal DISA numbers and make fraudulent calls. They also use sophisticated software packages to call a company's system and try to establish on which numbers a modem exist.

They will then try calling these modems and try to hack into the system using various methods.

The firm says that companies that publish toll-free numbers are most at risk as calls to these are free to incoming callers. And it fears that the popularity of the Internet allows a hacker to easily send information to a large community, so others can then make fraudulent calls.

The Tracker system is billed as monitoring calls made online to check for hacking activity and can also produce reports offline which can be used to analyse all telephone activity.

In use, a Tracker box is fitted to the call logging port of every PABX telephone switch to be monitored. It can store all call records output by the PABX for later analysis and can be used to search the incoming data against a number of user-defined criteria to look for unusual call patterns.

This change in call pattern can be used to produce an alarm if a hacker is attempting to break into a PABX or if fraudulent calls are being made. Call patterns in and out of working hours can be customised on a site by site basis.

The stored call records can be automatically collected by Foundation's Eclipse Call Management System each night. Management reports can be automatically produced and these can be analysed to check for fraudulent traffic.

Contact Foundation Data Systems on tel: +44 (0)1425 270333, fax +44 (0)1425 270433; e-mail: sales@fdsl.demon.co.uk

Computer to find abducted children

A computer system has been developed to help law enforcement agencies find missing children in the most critical first four hours after an abduction.

The TRAK Media Station Package is a computer system capable of scanning, storing, copying, receiving and sending faxes.

Bob Asquith founder of the TRAK system said: "We are a grassroots organization and we want to get anyone and everyone involved to help bring these systems to local police stations.

"From tragedies like the Polly Klass abduction and murder, law enforcement agencies have learned the first four hours after an abduction are critical.

"After that time the likelihood of a positive recovery is drastically reduced. The TRAK system is built around a massive response within the four-hour window.

"The real situation is that high-tech for most police departments is a fax machine and copier. That is just not going to get the job done."

Behind the system is the idea to move quickly in a four-hour window to get images and critical data not just to on-duty police officers and other law enforcement agencies, but to an entire community.

Asquith, formed SocialTech Inc., a not-for-profit corporation in Burlingame California. "Law enforcement agencies in most cases do not have the money to buy these systems. We have to give them away in order for TRAK to be in the right hands," he said.

By the end of 1997, he says approximately 175 TRAK systems will be deployed. More than 17,600 installations are needed to create a nationwide "immediate response" network.

More information is available at http://www.trak.org .

Cyber investigation firm launch in US

A UK firm which specialises in finding and analysing computer evidence has expanded to operate in the US.

London-based Computer Forensic Investigations Ltd will help companies, lawyers and accountants to uncover hidden data on a computer's hard drive which could be central in any prosecution or civil action.

Chief executive officer of the firm Tim Allen said: "In any investigation, and particularly those involving fraud, electronic data found on computers can provide the key to a successful prosecution.

"However, to get access to the critical information, which often lies hidden, the hard disks of the computers associated with the fraud and the floppy disks used by the suspects have to be copied in such a way that any information recovered will be suitable as evidence in court.

"The key to solving today's high-tech cases is to retain the evidential integrity of the data, otherwise subsequent analysis may be worthless."

The firm uses the proprietry DIBS® disk imaging backup system, developed by UK company Computer Forensics, to retrieve and analyse the data. Its makers say it works even if the information has been disguised, encrypted or deleted and that it does not compromise or affect the orginal system hardware or software in any way.

Computer Forensic Investigations

resident Peter Verreck said: "Already umerous criminals have been caught and nillions of dollars have been recovered hanks to this system.

"A common reaction when criminals re tipped off that they are fraud suspects s to tap away at the PC and try to delete whatever they can as quickly as possible. Unfortunately for them, we can recreate deleted files quite easily."

The firm can be contacted on +44 (0)171 353 3777 or by e-mail at nfo@computer-forensic-inv.com

Fighting Net hate

Bell Atlantic has joined with the civil rights groups to launch a new World Wide Web site to combat the escalating problem of hate speech on the Internet.

The firm has teamed up with the Leadership Conference on Civil Rights and the Leadership Conference Education Fund to set up a Web site offering advice and help.

Bell Atlantic chairman and chief executive officer Ray Smith said: "We saw an opportunity to join forces with the civil rights community to counter the frightening espousal of hatred and violence against Americans because of their race, gender, religion, or sexual orientation."

LCCR Executive Director Wade Henderson said the idea to create an Internet site was also triggered by the proliferation of Internet hate speech by groups such as the Ku Klux Klan and the White Aryan Resistance.

Such hate groups have become more sophisticated in recruiting, and the number of hate sites on the Internet has more than doubled to 250 in the last year.

The LCCR/LCEF Web site will provide up-to-date information on hate crimes around the country, community, legal and law enforcement strategies to address those crimes and materials for young people, parents, and teachers.

Stronger encryption program

A new software toolkit has been launched by US firm Pretty Good Privacy Inc which will allow non-computer experts to build security into applications.

Launching PGPsdk, the firm said it was the strongest commercially available product and could be used without any expertise in cryptography.

The system features 128 bit technology as well as encryption, decryption, digital signature and verification and is available for development on Windows 95, NT, Macintosh, Sun Solaris Sparc 2.5 and Linux platforms.

PGP president Phil Dunkelberger said the system would boost confidence in trade on the Internet as well as help those who rely heavily on sensitive electronic communication.

For more information, the firm's website is at http://www.pgp.com

Web based crime fighting tool

A new service which lets law enforcement agencies share important information on the Internet has been launched in the US.

The Bastille project, which will come online in February next year, features secure and encrypted databases accessible only by the relevant groups who subscribe.

Developers of the service, GTE Corp, say that with just a few mouse clicks officers and detectives can search for information including specific offenders, drug gangs, suspects, missing children, crime blackspots and sex offender release notifications.

Dan Jensen, vice president of GTE Enterprise Solutions said: "Bastille will use the Internet to virtually unify our nation's law enforcement efforts in the war against drugs, and delivers a cyber-knockout punch to criminals and gangs."

Dave Watkins, general manager of law enforcement services for the firm, said: "It gives law enforcement officers a secure forum to exchange information with individuals, specific groups or other agencies through information broadcasts, news groups, officer to officer e-mail and remote mobile access.

"Since the content of Bastille will be produced by law enforcement agencies, the service will be of greatest benefit as more and more agencies subscribe to the service, broadening the base of case information that is stored in the databases."

Already about a dozen Texas law enforcement agencies have begun using the system as part of a six-month trial.

Membership of the scheme costs $199 per month, which includes the software installation and set-up, training and technical support, as well as a 28.8 kbps modem/smart card reader. Agencies who sign up for a three year period will receive 200MMX PC system as well as a ten per cent monthly discount.

For more information contact GTE on +1 813 273 6900 or send e-mail to info@admin.bastille.com

Private eye on the Net

An Internet site has been set up to help people find out the truth about others they meet online.

The service, run by a Californian lawyer in the US, aims to help Net users check whether others are really who they claim to be.

There have been numerous cases of people using the anonymity of cyberspace to lie about their names, addresses, occupations, intentions and even their sex.

The WhoIsShe.com and WhoIsHe.com Web sites, was set up by Linda Alexander, a San Diego attorney, who charges $75 for a basic inquiry.

A detailed questionnaire is at each site to provide as much information as possible about the subject to be targeted.

Alexander said: "Everything I find out is public information. Finding out what people want to know is all from public records, but it takes time and you do have to know where to look.

"Just call me the Sherlock Holmes of the Internet. I feel this is an important service, something that should be done sooner not later."

Citing examples of her investigations, she said: "One woman met a man on the Internet who told her his wife was killed in a car accident. She turned out to be still alive. And another claimed to be a doctor, but wasn't."

She added: "Lies are lies whether they are online or on paper." To access the service go to http://www.WhoIsShe.com and http://www.WhoIsHe.com .

Threat of hackers

Scare stories about hackers who break into government and military computers have been a favourite Hollywood theme. But the findings of a US investigation has reavealed that the threat is very real. Paul Johnson reports.

The United States is vulnerable to computer based attacks and authorities have to increase security measures, according to a top level report.

A presidential commission says that the major computer networks and systems are vulnerable to terrorists and hackers who could wreak havoc with the government and the economy.

The Commission on Critical Infrastructure Protection has delivered a classified report to the White House which says the US's dependence on computers for its security, business and way of life make the country increasingly vulnerable to computer attacks that could easily wipe out communications and electricity grids.

The report said: "National defense is not just about government anymore, and economic security is not just about business anymore.

"Today, the right command sent over the Internet to a power generating station's control computer could be just as effective as a backpack full of explosives and the perpetrator would be harder to identify and apprehend.

"Infrastructure assurance must be a high priority for the nation in the Information Age. With escalating dependence on information and telecommunications, our infrastructures no longer enjoy the protection of oceans and military forces. They are vulnerable in new ways. We must protect them in new ways."

And the report said as more people became computer literate in society, the numbers capable of planning and executing a cyber attack grew as well.

It said: "The wide adoption of public protocols for system interconnection and the availability of hacker tool libaries make their task easier.

"While the resources needed to conduct a physical attack have not changed much recently, the resources necessary to conduct a cyber attack are now commonplace.

"A personal computer and a simple telephone connection to an Internet service provider anywhere in the world are enough to cause a great deal of harm."

The commission recommended setting up a programme across the country to educate people from all walks of life about the potential threat and what measures can be taken to counteract it.

It also said that the existing laws should be changed to cope with hackers using the Net.

"Law has failed to keep pace with technology. Some laws capable of promoting assurance are not as clear or effective as they could be," the report said.

It added that because altering the legislation would be a "lengthy and massive undertaking," measures would have to be taken to jump start the process.

"We identified existing laws that could help the government take the lead and serve as a model of standards and practices for the private sector. We identified other areas of law that can enable infrastructure owners and operators to take precautions proportionate to the threat."

The commission recommended doubling the $250 million the federal government now spends on research into beating hackers and it is reported that this $500 million will be increased by $100 million each year until $1 billion is dedicated to it by the year 2004.

It is thought much of the money would go to universities and private firms to fund research into ever more sophisticated intrusion detection devices.

White House spokesman PJ Crowley said that a task force composed of representatives from several government agencies will review the commission's report and come up with their own findings.

And an advisory committee headed by former senator Sam Nunn and former Deputy Attorney General Jamie Gorelick will work with the private sector on ways to stop criminals using computers in cyber attacks.

At a recent conference on computer security, commission chairman Robert Marsh said misuse of the Internet posed a real threat. He said: "While a catastrophic cyber attack has not occurred, we have enough isolated incidents to know that the potential for disaster is real and the time to act is now."

US Defence computers under attack

Hackers broke into more than 250 US Defence Department computers last year and the number is predicted to double this year.

The startling figures were revealed by a senior US intelligence official and will add weight to the call for public authorities to take a tougher stance on security and computer crime investigation.

Air Force Lt Gen Kenneth Minihan, director of the National Security Agency, told the Association of Former Intelligence Officers' annual convention that people should be afraid of computer misuse.

He said: "We have evidence that our known network and computer communications vulnerabilities are being exploited by attackers."

The NSA is regarded as a "secret" government body which monitors global communications.

Minihan did not identify the culprit or culprits or say what information had been stolen or what damage to systems had been done.

In his remarks to the convention, he said mounting reliance on computers had heightened vulnerability to "adversarial nation-states" as well as guerilla groups, narcotics traffickers and organised crime syndicates.

He said that the 1.3 million local area networks in the US are being threatened by both network sniffer programs which monitor online communications, and by attack programs which could disable systems.

And he claims that the US "will eventually pay for" building its information infrastructure "on a poor foundation" unless it increases computer system protection.

Court reports

Hacker case dropped

Charges in the UK against an alleged computer hacker who was said to have nearly started a war between North and South Korea after gaining access to US military computers have been dropped.

At an appearance at court in London, prosecuting solicitor Andrew Mitchell said that it was not in the public interest for the case against Matthew Bevan, aged 23, to now continue.

Bevan's alleged colleague, Richard Pryce, now aged 19, of Colindale in London, has already been fined £1,200 by Bow Street Magistrates Court, over the unauthorised accesses, which prosecutors said occurred in 1994.

While Pryce elected to be tried at the Magistrates Court, Bevan opted for trial by jury in the higher Crown Court, where his charges were dropped.

At Bevan's preliminary hearing, he was alleged to have gained unauthorised access into US military computers and into the computer systems of the North Korean defence systems.

This led the Koreans to assume that it was the US military that had gained access to its computer systems, as part of the preparations for a war against North Korea and the online incidents sparked a serious diplomatic incident.

After Bevan's case was transferred to the Crown Court, Judge Geoffrey Rivlin was told that the proposed trial would last several months and almost certainly result in classified information being revealed in a public courtroom.

Coupled with the need for several thousands of pages of documentation and at least 10 witnesses to fly in from the US, the prosecution was asked to "consider its position."

According to Peter Sommer, a senior research fellow at the Computer Security Research Center at the London School of Economics, who acted as defence expert to both Pryce and Bevan, the case failed because the UK prosecution authorities recognized that going to full trial would be both very expensive and have a high chance of failure.

He said: "The expense would come from the length of trial and the numbers of USAF personnel and others who have had to be flown into London. He added that he believed that a lot of the US evidence would have collapsed on detailed scrutiny.

He said: "The US cyber sleuth teams simply did not understand the difference between conducting a technical investigation and producing robust admissible evidence. Perhaps that's because they were service personnel and not police.

"The US authorities were refusing access to the source code of some of the Internet monitoring software they were using, essential if its reliability is to be fairly assessed, and the work of teams was being artificially summarised without any opportunity to test the original.

"Worst of all, having set traps to catch hackers, they neglected to produce "before" and "after" file dumps of the target computers.

"In a way I'm disappointed that there was so little opportunity to test the technical evidence as the two cases were something of a test-bed for new techniques in computer forensics."

US man gets jailed for online porn

A man has been sentenced to one year and three months imprisonment on a federal child pornography charge.

Robert Lightfoot Jr, 37, from Plainville, Massachusetts, was jailed by US District Judge Edward Harrington on a charge of having received child pornographic images contained in computer files on or about February 12, 1996, US Attorney Donald Stern said.

In addition to the prison term, Judge Harrington also ordered forfeiture of two computer systems which Lightfoot used in the course of the offence.

And he ordered Lightfoot to participate in psychological treatment, and to have no unsupervised contact with minors during the three-year period following release from prison.

At an earlier hearing, a federal prosecutor told the Court that Lightfoot traded child pornography via newsgroups offered by several online services, including Prodigy and America Online, as well as directly with individuals first contacted through such groups.

The three images, which are the subject of the indictment, depict prepubescent children engaged in explicit sex.

"Computer transmission of child pornography, particularly via online services and the Internet, has revitalized a very troubling means of victimizing children, both those who are depicted in the pornography and those who are preyed upon using such images to break down inhibitions," Stern said.

"The ease with which this crime is committed is no defence," he said. "The federal sentencing guidelines treat child pornography in general very seriously, and computer transmission more so."

The investigation against Lightfoot was conducted by the US Customs Service and was prosecuted by Assistant US Attorney Jeanne M. Kempthorne, deputy chief of Stern's Economic Crimes Unit.

- Earlier this month, another Massachusetts man, Ronald Langevin, was sentenced to two years and nine months in prison by US District Judge George O'Toole after Langevin pleaded guilty to a charge he had unlawfully possessed child pornography.

Langevin also used America Online to obtain and transmit the pornographic images he was charged with possessing. Along with the prison term, Judge O'Toole also ordered that Langevin's computer equipment be forfeited to the government.

The case, investigated by the US Customs Service and prosecuted by Assistant US Attorneys Timothy Feeley of Stern's Major Crimes Unit, and Shelbey Wright of Stern's Asset Forfeiture Unit, was part of Operation Rip Cord, an 18 month, joint sting operation first launched by New York State Attorney General Dennis Vacco (see news on page seven).

- A New York man also pleaded guilty to charges that he transmitted child porn images over the Internet.

Martin Dano, 35, of West Bloomfield, New York, pleaded guilty before Ontario County Court Judge James Harvey in Canandaugua, New York, to a single count of "Possession of a Sexual Performance by a Child," a class "E" felony punishable by up to four years in prison. Sentencing will be on December 17.

Law and secure computing

The legal liabilities of networked organisations in regards to computer crime and hacking

By Jimmy C. Tseng

Abstract

Computer crime and hacking has resulted in a number of new laws in order to cope with this phenomenon. However, the number of reported incidents, and successful prosecutions are still very low, perhaps due to a lack of understanding of the law, the legal liabilities, the methods of investigation and the preservation of evidence in this regard.

It is believed that better education and awareness will result in better prepared networked organisation, followed by more legal proceedings in the future, but the current priority is to promote awareness of legal obligations of both organisations and individuals prone to casual hacking.

This is to prevent the sacrifice of non-malicious hackers in order to set an example to the rest of society in the transformation towards a networked society.

1. Introduction

The importance of computer security and integrity needs no further elaboration, organisations that have fallen victims to computer crime found out about these threats the hard way. They include financial loss (including loss of revenue and recovery costs), loss of consumer confidence, loss of data integrity, and incurring damages to a third party.

Many of the victims of computer crime have chosen not to report them, significantly limiting the amount of information available [1]. However, the rapid growth of wide area networks especially the Internet, makes the potential for computer crime, especially computer hacking, even more disquieting.

The high profile of computer hacking in the 1980s seems to have abated after new laws were introduced in both the UK (Computer Misuse Act 1990), US (Computer Fraud and Abuse Act 1986) and in other countries.

Several high profile crackdowns focused the public's attention on hacking (Sterling, 1993) (Hafner, 1992), and other forms of computer crimes (Essinger, 1990). What is the current status of computer hackers (Newsweek, 1995)? What is it that makes hacking stories both inspirational and disgusting at the same time (Sterling, 1993)? Are hackers now happily constrained by their own set of self-imposed ethical standards of behaviour[2]? Has the new laws and law enforcement persuaded them on the proper path[3]? Or have they found working for the authorities more rewarding (Roush, 1995)?

A wide range of social and legal issues have to be considered in order to answer these questions concerning the future of the networked society. Computer hacking is an interesting social phenomenon, characterised by a fundamental urge of individuals to gain control in the information age (Jennings, 1992).

The wide publicity of computer hacking gives the general public an impression that computer security is defenceless against the mystifying cult of hackers. Even with the increasing realisation that the network behaviour of individuals are also susceptible to social norms and legal liabilities, the general feeling is that new legal and ethical systems are not yet in place, and the Robin Hoods of the 'electronic frontier' are to be tolerated (Barlow, 1993).

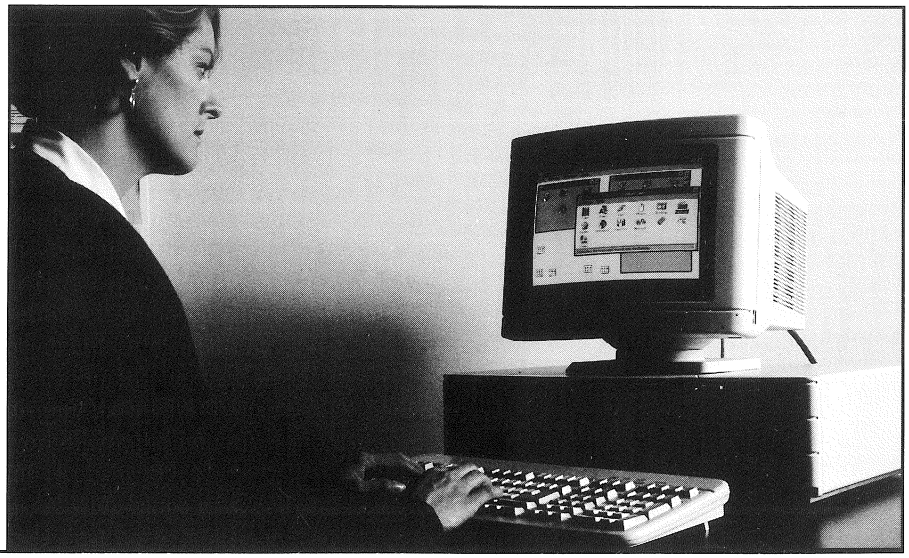
The legal dimension by itself is insufficient, law itself needs reform in order to fit changing social situations (Katsh, 1989). The specific and revolutionary features of information technology and the social phenomena of network society has to be considered (OECD, 1986) (EFF, 1995).

Much has been written about the security aspects of computer crime and hacking (Pfleeger, 1989) (Fites & Kratz, 1993), and numerous textbooks cover the criminal offences inflicted by hacking (Lloyd, 1993) (Bainbridge, 1993).

Most academic, commercial, and legislative resources have been devoted to protecting the supposedly benign, and naive organisations that are victims of computer hacking.

This article will focus on the legal liabilities of networked organisations that have reasons to believe they are susceptible to computer crimes, especially those initiated by unauthorised access and hacking.

Rather than addressing computer hackers as the mysterious 'computing underworld' (Sterling, 1993) (Hafner, 1992), and placing all the social burden on 'deviant' hackers, organisations



should, review existing security policies and procedures, and possibly re-define them if they are to receive the full support of the law.

2. Legislation and law relevant to computer crime

Statutes in both the UK (The Companies Act 1985, The Financial Services Act 1986, The Banking Act 1987, The Building Societies Act 1986) and the US (The Foreign Corrupt Practices Act 1977) [4] dictate the legal obligations of management to enforce appropriate levels of computer security.

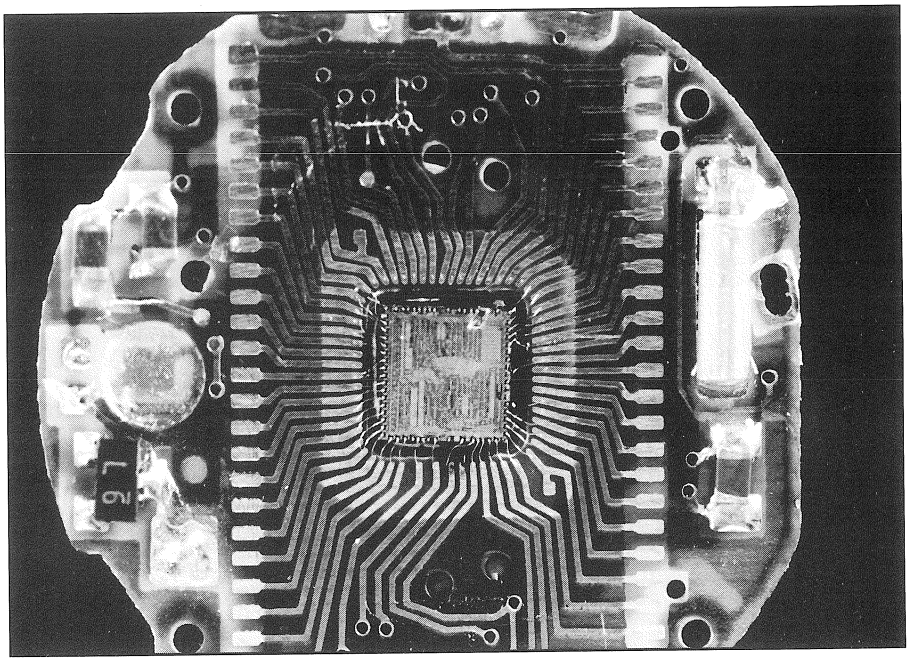
Other statutes have been introduced in the UK (Computer Misuse Act 1990, UK Data Protection Act 1984) and in the US (The Computer Fraud and Abuse Act 1986, The Electronic Communications Privacy Act 1986, The Computer Security Act 1987, The Credit Card Fraud Act 1984, and various state legislation) to prosecute individuals for computer misuse. Laws relating to admissibility of computer generated evidence also had to be re-interpreted in the new electronic media (UK Police and Criminal Evidence Act 1984, UK Criminal Justice Act 1994).

A quote from an OECD Information Computer Communications Policy report best describes the new economic value of information and legal attempts to control this phenomenon:

"One of the factors inherent in information and telecommunications technologies is that their misuse can leave no trace; but law is traditionally based on texts and material evidence of acts which, for computer-related crime, are often unavailable.

"This makes it difficult to assess the scale of and to detect and prosecute computer-related crime. The amendments of laws on the admissibility of evidence to take the supporting technology into account, could assist in prosecuting.

"These difficulties may influence Member countries in deciding which procedure to choose for initiating proceedings: to act only in the lodging of a complaint or to prosecute automatically. The victim may be no clearer than the offender of his rights and obligations and



may not be prepared to divulge information if the consequence could be to threaten a market position or commercial credibility.

" Many victims feel that they have not taken all the necessary measures to protect their new computer-based asset, on cost-benefit grounds. This is borne out by the lack of success of computer-related crime insurance." (OECD, 1986)

Management in networked organisations are legally responsible for an 'adequate' level of security for their information systems. It often turns out that the 'victims' of computer hacking (networked organisations) are also at fault since they have not provided 'adequate' security measures required by the law.

Instances of computer crime undermines management's credibility to uphold it's stewardship responsibilities. This is complemented by the fear of a public relations fallout, resulting in lack of consumer confidence (Gelinas, Oram, & Wiggins, 1990). Quoting David Stang, president of Norman Data Defense Systems: "You feel dirty after a hacker attack or a computer virus infection, like you've done something wrong, you don't want to tell anybody, which winds up affecting the reporting of incidents." (Roush, 1995)

If and when incidents do get reported, not all investigative agencies are adequately trained to "prevent further damage, limit the losses incurred, find out what went wrong, identify the perpetrator, and preserve the evidence for a successful legal prosecution" (Smith, 1993).

Furthermore, investigation of computer crime will "inevitably be pitted against time and operational pressures, making the proper handling of the investigation and preservation of evidence even more difficult" (Smith, 1993).

For networked organisations to be fully protected by the law, management and security staff should be aware of their legal liabilities under both criminal law and civil law. This issue will be discussed further in the next section.

3. Legal Liabilities of Networked Organisations

Criminal liabilities are concerned with the legal obligations of citizens to the state. Management in a networked organisation is liable for assuring the security of the company's financial accounts, and any personal information held on computer systems.

The nature of criminal cases means that a great deal of time is spent on deciding whether evidence is admissible or not (Smith, 1993), and even then, successful prosecution does not usually result in compensation to the party that suf-

fers damages.

However, they are conducted under public expense, providing useful evidence to support a claim for civil wrong doing (Chalton, 1990).

3.1 Accuracy and Integrity of Computerised Company Records

Companies are required under section 722 of the Companies Act 1985 to take adequate precautions against the falsification of accounting records, including those of a computerised nature. If accounting records are computerised, then appropriate physical (e.g. access controls), technical (e.g. audit trails) and administrative controls (e.g. separation of duties) should be in place.

Failure to keep proper accounting records under section 722 could constitute a breach of section 221, which would be an offence under section 223 unless management act honestly and the default is excusable under the circumstances of the business (Kelman, 1995).

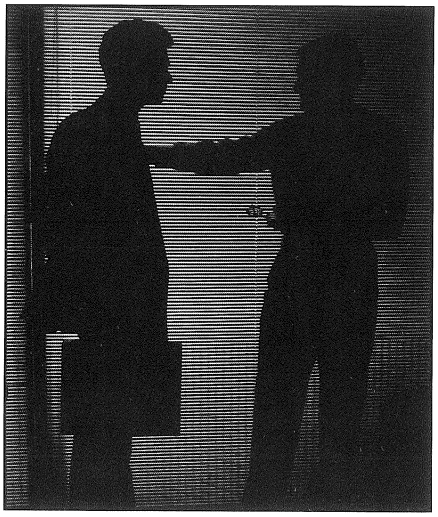
The Financial Services Act 1986 also has provisions regulating the use of computerised accounting information systems. Requirements include "an organised systems development methodology, an up-to-date documentation of systems, effective change control procedures and adequate testing of system changes, effective access control software, and adequate up-to-date and well tested disaster recovery plans". Self-regulatory organisations are also set up under the act to monitor compliance (Smith, 1993).

The Bank of England and the Building Societies Commission have issued notes to banks (Guidance Note on AORICS, Accounting and Other Records and Internal Control System) and building societies (Prudential Note) providing guidelines on "system development risks, data entry errors, program modification errors, fraud, access to confidential information, internal controls, internal audits, and disaster recovery (or business interruptions)" (Essinger, 1990) (Smith, 1993).

The US Securities and Exchange Commission and the American Institute of Certified Public Accountants also issued similar security guidelines (see AICPA Statement on Auditing Standards No. 55) (Gelinas, et al., 1990).

Companies have another reason to place high priority on the integrity of their computer-based information systems. Under the Insolvency Act 1986, companies applying for an 'administrative order' in times of financial crisis to prevent creditors from dissolving the company will have to show the courts financial projections.

The government and court does not like bailing out 'failures', thus the security and integrity of all company records including the computer-based information systems should be well guarded and well maintained as an added precaution for business continuity (Kelman, 1995).



3.2 Protection of Personal Data

The principle that personal information on computers must be adequately secured under the Data Protection Act 1984 implies increased liabilities for organisations. The Act maintains that organisations holding personal data on living individuals in a form that can be automatically processed, unless exempt, must register itself as a data user to the Data Protection Registrar.

Failure to register carries a maximum fine of £5,000 in a Magistrates Court or an unlimited fine in a Crown Court. Registered data users must not contravene the eight Data Protection Principles. Failure to comply with the principles may result in a preliminary notice, followed by an enforcement notice (a time frame for a data user to comply with a breach in Data Protection Principles), a de-registration notice (a notice that a data user is no longer able to hold personal data without committing a criminal offence), or a transfer prohibition notice (a notice which prohibits the transfer of personal information to countries outside the UK).

Failure to comply with the notices is a criminal offence under section 5 of the Act. The organisation, it's directors and managers may all be liable. The organisation and the managers are liable under section 5 if they committed the offence knowingly. The directors are liable under section 20 if they had consented to the offence. Other senior officers may be liable due to neglect of ensuring adequate security (Bainbridge, 1993).

Data subjects can also claim damages against the loss or unauthorised disclosure of personal information under section 23 of the Act. Therefore, the networked organisation should take proper measures against unauthorised access and modification of personal data, as well as providing frequent audits and backups.

Due to reasons of personal privacy, national sovereignty and economic sovereignty, various nations have legal or administrative restrictions on Transborder Data Flow (TDF). The legal threats to networked organisations may come either from national data protection laws, or restrictions on export of data to countries without such regulation.

Organisations might resolve this difficulty either through a contractual clause with the trading partner, or by re-organising it's data processing activities (Walden & Savage, 1990).

3.3 Authorisation for Access and Modification of Data

The Computer Misuse Act 1990 does not impose statutory duties on networked organisations, but it does require employees and other users of computer-based information systems to understand fully the limits of their authority. All instances of misuse also have to be detected and properly logged at an early stage (Smith, 1993).

3.4 Admissibility of Computer-generated Evidence

Before the Police and Criminal Evidence Act 1984, the admissibility of computer generated evidence depended on 1)

whether the evidence was generated wholly by computer or with human involvement, 2) whether experts can testify on the reliability of the computer system, 3) whether it is the 'best evidence'.

Section 69 of the Police and Criminal Evidence Act 1984 now accepts computer-generated to be admissible unless there has been some human intervention in the computer process. Under such circumstances, a certificate will be required by the system manager stating that there are no reasonable grounds for believing the computer was used improperly, and the computer was operating reliably at all times, or if not, that the impairment could not have affected the accuracy of the evidence (Kelman, 1995) (Smith, 1993).

3.5 Civil Liabilities of Networked Organisations

Civil liabilities are concerned with the contractual rights and obligations of organisations (liabilities under contract) and liability to strangers, for example, negligence and breach of statutory duty (liabilities in tort).

They are governed mostly by common law, and may be incurred when management have not taken special precautions. Management should be aware that other than the criminal liabilities they may incur from computer crimes, or damages from computer crimes, the business can suffer seriously if the incident had affected other parties on the other side of contracts.

The injured parties can either affirm the contract, bring the contract to an end, or claim damages. Organisations may also be subject to claims for negligence if it can be proved that the organisation owed the defendant a duty to take care, and that it had breached that duty.

With the pervasiveness of computers in modern organisations, intrusions like hacking and viruses will very likely impair the operation of the organisation, resulting in civil liabilities. Adequate security should not be taken for granted, especially when life-critical systems are involved.

The admissibility of Computer Evidence under civil law is governed by the Civil Evidence Act 1968, which does not cover ad hoc reports or printouts of the system log unless they are regularly generated (Smith, 1993).

Organisations might consider leaving a regular trail of physical printouts as a consequence, in order to counter claims for civil liabilities.

3.6 Legal Liabilities of Computer Bureaux, EDI Service Providers, Network Service Providers and Bulletin Board Operators

A set of different issues and laws cover computer and telecommunication service providers, however, they are outside the scope of this article. The issues will be covered quickly in this section.

Computer bureaux and Electronic Data Interchange (EDI) service providers may have contracts specifying access and availability of their resources. For example, companies that have outsourced their information systems facilities, or multi-national corporations running electronic funds transfer systems, may find 24 hour uptime to be essential.

The Computer Misuse Act 1990 does not impose statutory duties on networked organisations, but it does require employees and other users of computer-based information systems to understand fully the limits of their authority. All instances of misuse also have to be detected and properly logged at an early stage (Smith, 1993).

3.4 Admissibility of computer-generated evidence

International laws and regulations related to EDI have separate security requirements which organisations will be liable to once they sign the contracts [5] (Carr & Williams, 1994).

Service providers and bulletin board operators may also need to protect themselves against infringement of copyright (when pirate software is stored on their system, or distributed through their network by a third party), or the potential liability for defamation and libel (when controversial remarks are stored on their system, or distributed through their network).

The following advice is based on the possible threat of computer crime and hacking and the legal liabilities:

1) specify explicitly the levels of authorisation for each task and job role,

2) keep system logs in order to establish the computer system's reliability,

3) re-examine internal controls in order to reduce human errors to a minimum,

4) implement separate access controls especially for sensitive personal data,

5) keep audits trails to prove the accuracy and integrity of computer-based information, it may also be the crucial evidence that is needed to link an offender to an otherwise unrecorded access, duplication or modification transaction,

6) consider keeping a regular trail of

paper printouts for physical backup and evidence in civil courts,

7) balance operational needs and the preservation of evidence in the disaster recovery and contingency plans.

5. The Role of Education and Awareness in the Deterrence of Computer Hacking

Organisations that have prepared themselves for the computer crime and hacking need not be trigger happy. Computer hacking should not to be forgiven, but there are reasons to believe that the motive behind many hacking cases documented in the past few years have not been malicious.

It is better to promote awareness of socially acceptable behaviour and to educate others on the legal reforms that have taken place in this age of transformation. An unmistakable method would be to post a notice of liability on login screens instead of 'Welcome to Super Computer' messages.

Even though sound security principles are against such publicity, i.e. advertising highly sensitive systems as such by issuing a warning notice prior to login, but casual hackers should be aware that mere login attempts on systems located in the UK constitutes a basic offence under the Computer Misuse Act 1990. The Act also applies "whenever an alleged offence is conducted from or directed against the UK".

Information on legal liabilities in various countries should be made widely available. Service providers and information providers should make the legal liabilities that apply in that country available, and if extradition applies for that offence (currently applies only to indictable offences under sections 2 and 3 of the Computer Misuse Act 1990), the legal liabilities that apply in other countries should also be widely available (see Bainbridge 1993 pp. 172-173, Lloyd 1993 pp. 188-190).

Before such legal information is harmonised, which seems highly unlikely, the distribution of such legal information should be wide-spread and well publicised, otherwise computer hacking will always be regarded by techies as casual adventuring.

The international aspects of computer networking makes decisions on jurisdiction difficult. In spite of attempts to harmonise computer-related crime and penal law in the Organisation for Economic Co-operation and Development member countries (OECD, 1986) and the European Community, current differences in law undermines fair sentencing.

For example, a defamatory remark made on the US network is distributed around the world to the UK, the plaintiff in this case can select the country of his choice to sue. English laws make it easier for the plaintiff to recover damages, while US laws requires the plaintiff to prove the defendant guilty (Conaill, 1995). Other issues of fairness and justice are bound to jump out as we progress towards the future networked society [6].

6. Conclusion

Organisations today can no longer afford to remain isolated from the network society. Firewalls and other technical controls are only as good as the personnel who set up and monitor them. The networked organisation with all its frightening consequences are increasingly becoming a reality.

In answer to the question raised in the introduction about the current status of the hacker culture, has hacking lost it's significance? Do organisations still need to protect against computer hacking? Definitely yes, evidence shows that hacking in the future will become even more serious, sophisticated, and malicious[7] (Roush, 1995).

Before 1986, many nations did not have laws for deterring computer hacking (OECD, 1986), but the combination of new laws, law enforcement experience, and a series of high profile prosecutions had an immediate impact on the US hacking community, and through worldwide publicity, many other parts of the world. Law reforms, in the UK at least, have made the legislative position on computer crimes and hacking quite clear.

Explanations of why organisations that have become 'victims' to computer crime and hacking have not resorted to the law was highlighted in section 2 of this article. Laws relevant to the provi-

sion of adequate security, and other legal liabilities that organisations may incur in their adoption of computer and networking technology was discussed in section 3.

It is hoped that organisations can use this knowledge as a starting point for re-examining their information systems security in order to receive the full protection of the law, an example of this was listed in section 4.

And finally, in section 5, the need for education and awareness of the new laws relating to networked computing was discussed. Law enforcement, organisations, and individuals need more exposure to these laws before comprehending fully their legal obligations and liabilities. In the future, as the legal liabilities of all parties are better understood, more prosecutions and more arbitration based on the law will follow.

It has been said that prevention is better than cure, but awareness of the law is even better than prevention. Awareness of legal liabilities of all parties involved provides a useful guideline for self-regulation, resembling a national information security policy.

The network society still faces many more challenges on what constitutes acceptable behaviour on the network. Society should not hesitate in reforming existing laws and legislating new ones to protect and to bring about justice. But ultimately, it will depend on every member of society to follow the law, by fulfilling their obligations with an understanding of their legal liabilities.

Appendix A : Further reading on the legal liabilities of computer hacking

Computer Misuse Act 1990, Data Protection Act 1984, Telecommunications Act 1984, Copyrights, Patents, and Design Act 1994

Appendix B: Further reading on computer crime law in other countries

OECD, (1986). Computer-related crime: analysis of legal policy. (ICCP No. 10) pp. .7-71

Smith, M. (1993). Commonsense Computer Security (2nd ed.). McGraw-Hill. pp. 268-274

Footnotes

[1] Donn Parker (US) estimates that only 20% - 25% of all computer crimes are reported.

[2] Those interested in so called hackers ethics can read "Secrets of a Super Hacker", or "The Hacker Handbook III".

[3] Those interested in the hacker-law enforcement-civil libertarian relationship should read Sterling's book "The Hacker Crackdown", connect to the Electronic Frontier Foundation's WWW server at www.eff.org.

[4] The international nature of computer crime and hacking creates problems for jurisdiction, hence law in different countries may have to be considered. Due to space restrictions, only the relevant UK and US statutes will be listed in this section, but the rest of this article will focus on the relevant UK laws only. European readers would also be interested in checking the relevant European Community Law. Please refer to Appendix B for references to related legislation in other countries.

[5] Those interested in Electronic Data Interchange (EDI) might like to look at the technical security in UN/EDIFACT User Manual, and the contractual arrangements under UK EDI Association 'Standard Interchange Agreement' (SIA) and US American Bar Association 'Trading Partner Agreement' (TPA).

[6] Computing professionals may not be responsible for shaping these issues into law, but they are responsible for communicating these issues to other members of society. When in doubt, socially responsible computing professionals should try to balance the four ethical issues in the computing profession, accuracy of information, personal privacy, access to information, and intellectual property rights.

[7] The future hackers will probably not be naive and persistent teenagers since much of the thrill of accessing undisclosed information has been dampened by the widespread availability of online information today. However, the network society still faces many challenges on what constitutes acceptable behaviour on the network, e.g. intellectual property rights, privacy rights, responsibility for defamatory remarks, etc. It is the proposal of this article that the purpose of law is to serve individuals (including hackers) and organisations, hence the need to educate, understand, develop and follow legal constraints.

References

Bainbridge, D. I. (1993). Introduction to Computer Law (2nd ed.). Pitman Publishing.

Barlow, J. B. (1993). Law and disorder on the Electronic Frontier.

BCS SIG Law (1995). Legal issues on the Internet, Lecture given at City University, 16 Feb., 1995

Carr, Indira and Katherine Williams. Computers and Law. Oxford: Intellect Ltd., 1994.

Chalton, S. (1990). An introduction to the legal liabilities of information producers. In C. Edwards, N. Savage, & I. Walden (Eds.), Information Technology and the Law (pp. 4-23). Macmillan.

Conaill, C. O. (1995, May 1995). Crime on the Net. Internet, p. 32-34.

Cook, T. (1990). Facilities Management and Other Computer Services Contracts. In C. Edwards, N. Savage, & I. Walden (Eds.), Information Technology and the Law (pp. 130-141). Macmillan.

EFF (1995). Electronic Frontier Foundation. http://www.eff.org.

Essinger, J. (1990). Computer Security in Financial Organisations. Elsevier Science.

Fites, P., & Kratz, M. (1993). Information systems security: a practitioner's reference. New York: Van Nostrand Reinhold.

Gelinas, U. J., Oram, A. E., & Wiggins, W. P. (1990). Chapter 5 Controlling Information Systems: A Control Framework. In Accounting Information Systems (pp. 122-126). PWS-Kent Publishing.

Hafner, K. (1992). Cyberpunk.

Jennings, D. (1992). Unknown, referenced in Bruce Sterling's book, The Hacker Crackdown. .

Katsh, M. E. (1989). The electronic media and the transformation of law. New York Oxford: Oxford University Press.

Kelman, A. (1995). Legal Aspects of Secure Computing. Lectures given at the London School of Economics, Legal Aspects of Secure Computing course

Lloyd, I. J. (1993). Information Technology Law. Butterworths.

Newsweek (1995, February 27, 1995). InfoMania. Newsweek

OECD, (1986). Computer-related crime: analysis of legal policy (ICCP No. 10). OECD.

Pfleeger, C. P. (1989). Security in Computing. Prentice-Hall.

Roush, W. (1995, April 1995). Hackers - Taking a byte out of computer crime. Technology Review

Skinner, D. (1994). Audit Commission Report 1994, Lecture given at the London School of Economics, Information Systems Security Colloquium

Smith, M. (1993). Commonsense Computer Security (2nd ed.). McGraw-Hill.

Sterling, B. (1993). The Hacker Crackdown.

Walden, I. (1990). EDI and the Law. In C. Edwards, N. Savage, & I. Walden (Eds.), Information Technology and the Law (pp. 239-251). Macmillan.

Walden, I., & Savage, N. (1990). Transborder Data Flows. In C. Edwards, N. Savage, & I. Walden (Eds.), Information Technology and the Law (pp. 121-129). Macmillan.

Many thanks to Jimmy Tseng and the London School of Economics and Political Science Computer Security Research Centre.

MS-DOS Partitions

Recent investigations into MS-DOS based computers revealed some interesting information concerning the partitioning process, with important implications for forensic computer investigators.

As most people will be aware, the idea of partitioning was introduced when the physical storage capacity of fixed disks began to exceed the electronic capability of the operating system.

The capacity limit of BIOS routines depends upon the size of the numbers used to access the disk at low level. Addressing was usually via a Track, Head and Sector address and the relevant maxima for Track, Head, and Sector were 1023, 15 and 63.

Because Tracks and Heads (but not Sectors) were counted from zero this meant that the maximum number of addressable sectors was 1024 x 16 x 63 or 1,032,192. Since each sector was (usually) capable of storing 512 bytes this put a top limit of 528,482,304 bytes.

At the time when the original PC BIOS was developed this was felt to be more than sufficient for future needs. As engineering technology improved and disk sizes increased some modification of the BIOS increased the number of heads that it could handle from 16 to 256 and thereby increased the maximum capacity to 1024 x 256 x 63 sectors or 8 Gigabytes.

The operating system capacity however, has a different limit by virtue of the fact that it needs to maintain an index of material stored on the disk. This is done by the 16 bit FAT system which maintains a maximum of 65,520 blocks of space.

The size of each block (or cluster) is set when the system is initially installed and depends upon the physical size of the disk. Thus for a small disk of around 100 Megabytes, each cluster will be 2048 bytes (or 4 sectors) and there will be around 49,000 of them.

Whilst this system is extremely flexible, it is very inefficient in its use of space. For example if a file is created to contain only 40 bytes of information it will be allocated a single cluster and the remaining 2008 bytes would be unused by the file and unavailable to the system.

As the size of the cluster increases, this inefficiency increases. Forensically this phenomenon can be useful since this slack space may contain information written to previous and long-since deleted files.

The maximum cluster size acceptable to this 16 bit FAT system is 64 sectors or 32 kilobytes and this places a maximum capacity of 65,520 x 32768 or 2,146,959,360 bytes (2 Gigabytes) on the operating system as a whole.

The original PC BIOS boot routine was designed to address just the first sector of a physical drive. The presence of a four-entry partition table then allowed operating system software to access different sections of the physical drive by partitioning the available space on the physical drive into a number of areas, each of which could contain a different operating system.

> "The presence of directory fragments and their cluster number can be a vital link"

Of course it is also possible to put the same operating system into several different partitions and for MS-DOS this would mean that each partition would be treated by MS-DOS as a separate drive each accessible by a separate letter of the alphabet. Since the letters A and B were reserved for floppy drives, the letters C to Z were available for the other logical drives.

In the first of the investigations mentioned at the start of this article, the target machine was a laptop containing an 82 Megabyte fixed drive with four MS-DOS partitions.

The case involved alleged hacking and phone cloning. The first and second partitions contained normal system and user software but nothing concerning the allegations.

A small amount of evidential material was extracted from active files on the third partition and the fourth partition (labelled BLANK) was empty of active files. A search of the unallocated space on all four partitions revealed a little more material but nothing very substantial.

However, on the second partition, there were traces of live subdirectory entries which contained the names of files which appeared interesting. Strangely these subdirectory entries were offset 1024 bytes into each cluster rather than right at the beginning and when they were reformatted for display they indicated cluster numbers around 38,000, far higher than the maximum on any of the four partitions.

Note that the primary entries in a subdirectory indicate not only the cluster number of the parent directory but also the number of the entry itself. The following table indicates the overall partitioning scheme and the cluster sizes in each partition (See figure 1).

It had been noted during initial examination that the cluster sizes were unusual but note that the maximum cluster number on any drive was 14327.

It was postulated therefore that what we were looking at were fragments of information from a time when the drive had been partitioned into a single drive with a cluster size of 2048 bytes.

If that were the case, the fragments pointed to areas that were inside the fourth partition. A little patient calculation and some adjustment for the incorrect cluster offsets revealed a whole subtree of directories and several ZIP files

Partition size	Cluster size	Maximum number of clusters
29 Mbytes	2048	14327
20 Mbytes	4096	9765
13 Mbytes	4096	3173

Figure 1

which were for the most part unfragmented.

These were extracted and examined and provided a wealth of evidence to support the charges. It also happened that one of the files contained a utility to re-partition a disk without losing live data.

When tested, it became apparent that this had been used on the machine and it was this which had produced the unusual cluster sizes.

The other investigation illustrated the other condition - where a multiple partitioned drive had been reconfigured to a single partition. Case information indicated that the drive had been re-formatted at least twice and system software re-installed each time.

Examination showed that the typical 0F6h filler byte had been written to all clusters above 13,000 or so. However, these filler bytes did not extend right to the end of the drive. Above where the filler bytes ended, fragments of live sub-directories were found.

The entries were again at an incorrect offset but this time pointed to much lower cluster numbers. Translation calculations were completed and this time indicated that at some time in the past, the drive had had a final partition of around 10 Megabytes.

Most of the files in this partition were intact and were recovered, providing excellent evidence. The history appeared to be that the drive was originally partitioned into two logical drives and the first drive had been unconditionally formatted without removing the original Master Boot Record.

This may have happened more than once. Later the MBR had been destroyed - thus removing the partition table - and the whole drive was then repartitioned and reformatted, this time with an ordinary format. Thus the contents of the final section (the original 10 Mbyte partition) remained for examination.

It is rarely necessary to go to such lengths as are described above to recover relevant information, but in cases where there is no evidence in live files and only tantalising fragments in unallocated or unpartitioned space, the presence of directory fragments and their associated cluster number can be a vital link in the evidential chain.

Hoax viruses

Usually it arrives in the email inbox with a long list of email addresses of fellow recipients, with a short note that begins "I just received this..." and continues: "perhaps you want to pass this warning on to others" or "is this for real?" or "please take note."

The text continues along these lines:

"WARNING!!!!!! If you receive an email titled "JOIN THE CREW" DO NOT OPEN IT!

"It will erase EVERYTHING on your hard drive! Send this letter out to as many people you can.....this is a new virus and not many people know about it!

"This information was received this morning from IBM, please share it with anyone that might access the Internet... (etc.)"

This is categorically a hoax. There are several sites on the Internet that explain the different hoaxes and myths, one being:

http://ciac.llnl.gov/ciac/CIACHoaxes.html.

Let me also state flatly that you cannot get a computer virus simply by reading email.

However, you can if someone sends you a file as an attachment, and it is a Microsoft Word file. If this file has the "concept" or a related macro virus, your version of Word can be infected.

The solution here is to view any word documents in WordPad (the Windows Notepad that comes with Windows 95), or to get a program such as F-PROT that will detect such Macro viruses (F-MACROW will remove them) and check the attached file first.

(See http://www.datafellows.net)

Also, if someone sends you an executable file as an attachment, be suspicious (singing or musical greetings cards or animations can be infected with a virus), if in doubt it is probably better to delete these unless you expect that they contain valuable information. Or, at the very least, scan them first with a recent version of F- PROT.

It has been said that more time is wasted over false alarms about viruses than by the real things, while the Concept macro viruses that target Microsoft Word and Excel programs are the most widespread viruses around these days.

But, to repeat, simply opening and reading an email cannot infect a computer system. If you use a recent version of an Internet browser, you will be alerted if there is any activity that might be dangerous.

Embedded ActiveX controls were a case in point, even if Microsoft has now suspended its ActiveX work.

This was the "feature" that caused visitors to certain alleged porn sites to have their modems disconnect and then place a long-distance phone call to Moldavia. This was started as a prank, but the perpetrator has had to reimburse the thousands of victims in a recent US court ruling, (see news pages).

The fact is that personal computing is more hazardous today in an increasingly interconnected world, and it can be difficult for novice users to determine what is a potentially dangerous activity and what is not.

Reading email is not, casually opening a Word attachment can be.

Finally, it is worth downloading F-PROT now anyway. This is free, for the DOS version, at least. Use it to check out your system.

If it finds a known virus infection, it will either shut down (if the virus is active in memory) so that the anti-virus program itself does not get infected, or if it is safe to run, it will pinpoint any infected files (which it will clean or disinfect for you).

Secondly, if you do have a virus in memory, you may well need to start the computer from a known, clean floppy disk. Making one should be the first thing you do after you buy a new computer system.

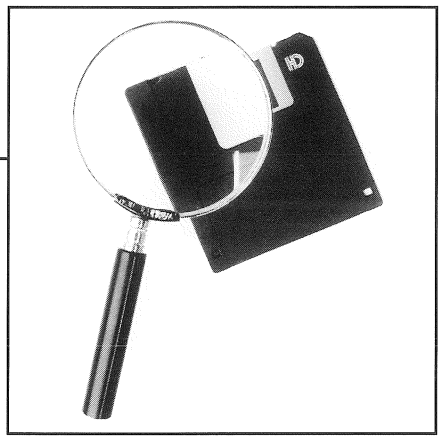
Get a blank, unformatted floppy disk, and place it in drive A.

Type format a:/s which will transfer the system files. Label this RESCUE DISK, along with the version of DOS you have, and at least you will be able to start your system in a known clean state (which it should be in when you buy it), for troubleshooting later.

And tell anyone who sends you warnings about the "GOOD TIMES VIRUS" or "AOL4FREE" or "JOIN THE CREW" not to worry.

By Tony Waltham

Forensic Q&A



Q ***During a search of an MS-DOS partition, I discovered what appeared to be the remains of a subdirectory cluster. Amongst those entries which were intelligible I found an entry which was exactly similar in every respect (including the starting cluster number) with another entry in a "live" subdirectory. How can this happen and is there any special significance to this?***

A It is quite usual to find traces of previous subdirectory clusters in both unallocated and slack space.

There are a number of reasons why this happens apart from the obvious one where a subdirectory has simply been deleted. Perhaps the disk has been defragmented at some time in the past.

If defragging is done without the wipe option, when a subdirectory is moved (i.e. copied) the original copy is left until something else is written to that space.

You do not say if the subdirectory entries were marked as deleted (with the first character changed to 0E5h). This is important because in MS-DOS a subdirectory cannot be removed until all the entries in it have been removed or deleted.

During defragging, individual entries are not "deleted" so if this is how your entries appear it may be the result of a defrag operation.

Under these circumstances, fairly obviously if the starting cluster is the same then the file must have been moved before the subdirectory.

However, if the matching entry is marked as deleted, this may be the result of a file move (rather than copy) operation. For example : within Windows' File Manager if a file is dragged from one subdirectory of a disk to a different subdirectory *of the same disk* the instruction is to move rather than copy the file.

The move process does not actually copy the file contents to a new location, instead it marks the original subdirectory entry as deleted and then creates a matching entry in the new subdirectory. Thus the result of such a move leaves two identical entries (apart from the first character) on the disk.

The significance of such observations must be taken in context but the presence of fragments of subdirectories might be useful in determining a sequence of events on a machine, particularly when compared with the results of cluster analysis.

Q ***Precisely what legal significance can be attached to the dates and times on files?***

A The short answer is none. The date and time of a file as recorded in the subdirectory entry is too easily changed without trace for it to be of any evidential value (particularly in 16 bit arenas).

You should also remember that when a file is copied, its date and time travel with it. However, a series of files within a subdirectory, containing similar dates but ascending times might be indicative of a multiple file downloading or copying session.

Analysis of the time differences between adjacent files compared to their respective lengths might even give some indication of the speed of the download.

It should also be mentioned that subdirectory dates and times are more difficult to change because when a subdirectory is created the current system date and time is written to three separate places.

Thus during a chronological analysis of a disk structure under MS-DOS, more weight should be given to the dates and times marked in subdirectory entries than those associated with files.

Once again, cluster analysis might help by highlighting any anomalies within the structure.

Q ***What is an "orphaned cluster"?***

A In MS-DOS, when a file is deleted the normal sequence of events is to first change the first character of the subdirectory entry to 0E5h (ASCII code 229) and then clear the chain of entries within the File Allocation Table back to zero to make them available again to the MS-DOS space allocation system.

Sometimes, after the subdirectory entry has been changed, the FAT is not cleared. This may be as a result of an unsynchronised cache buffer

or some misbehaviour within an alternative processing thread. The result leaves the original cluster chain still marked as allocated within the FAT but there is no associated owning file entry.

There is thus no way that MS-DOS can recover the space. The program CHKDSK has an option (using /v) to recover such orphaned clusters (Microsoft call them "unallocated chains") into files named with a characteristic FILE????.CHK where the ???? is a sequential number.

These recovered files will always be an exact number of clusters long and will appear in the root directory.

Once the chains have owning entries they can of course be deleted to recover the disk space.

Do not attempt to recover orphaned clusters on the evidential machine because the root directory entries may overwrite valuable evidence, do so instead on a rebuilt image of the logical drive.

Note also that there is a limit to the number of entries that the root directory will hold. Recovering large numbers of orphaned chains can overflow the root directory and prevent further recovery.

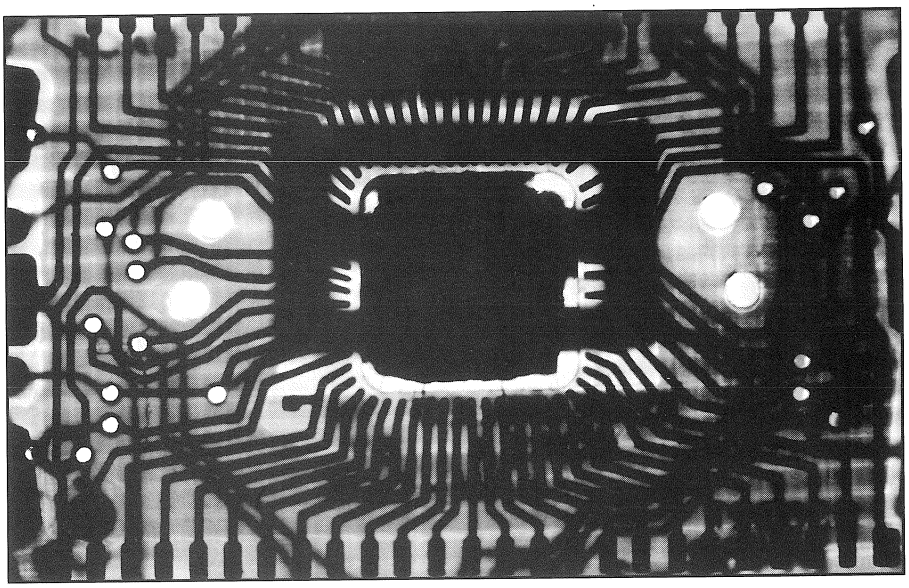
Q ***I have a number of ZIP files containing material which may be of interest on a particular case. When I attempt to UNZIP them I get a message saying : "Warning - skipping encrypted file!" How can I recover these files?***

A The short answer to your question is - you can't!

When creating ZIP archives, the PKZIP program has an option to encrypt each file with a password provided by the user.

Once zipped, these files cannot be unzipped without the password. There are a number of so-called Zip-cracker programs which will conduct a brute force decryption by trying all possible passwords until they find the one that works.

This approach will succeed but the problem is how long it takes to generate the test passwords. For example:



PKZIP will theoretically accept any of 251 different characters in a password.

So if the password were only 1 character long there would be 251 possibilities. With a password length of 2 characters there would be 251 x 251 possibilities and length 3 would have 251 x 251 x 251 possibilities.

Thus the formula for how many possible passwords there are of length *PWLen* becomes : 251^{PWLen}. As the password length increases this becomes a very large number as may be seen in the table (figure 1).

As may be seen from the times listed in the third column, this process can take an enormous length of time. Reducing the number of characters which may probably be in the password to 95 (26 lower case letters, 26 upper case letters, 10 digits and 33 symbols/punctuation marks) and arranging for several computers to work simultaneously on sections of the problem will reduce the times involved and knowing some of the probable characters is also a help.

However, this approach is generally impractical. Another approach involves testing millions of known words (a dictionary attack) - as noted above 15 million words can be tested in less than two minutes.

This will of course fail if the password is not a recognised word.

There are also certain cryptanalytic techniques that have been successfully applied in certain cases but these are outside the scope of this journal.

Length of password	No of possibilities	Time to generate all possibilities @ 150,000 per second
1	251^1 =251	-
2	251^2=63,001	0.42 seconds
3	251^3=15,813,251	1 minute 45 seconds
4	251^4=3,969,126,001	7 hours 21 minutes
5	251^5=9.96 x 10^11	76 days 20 hours 54 minutes
6	251^6=2.5 x 10^14	52 years 301 days
7	251^7=6.28 x 10^16	13,259 years
8	251^8=1.57 x 10^19	3,328,086 years
9	251^9=3.95 x 10^21	835,349,596 years
10	251^10=9.92 x 10^23	2 x 10^11 years

Figure 1 (^ denotes "to the power of')

Space trashers

By Jim Bates

I have recently been asked for comments and observations on a number of programs which in various ways try to prevent the operating system from leaving traces of user files dotted around the fixed disk in unallocated and slack space.

Marketed as "security software", these programs offer positive file deletion, slack space clearing and even swap file sanitation amongst their options.

Some require operator action whilst others can be installed as active background applications which monitor system activity and positively wipe any temporary or redundant file content.

In some cases the overwrite options offered would support a paranoia which would do credit to a third world dictator. Fairly obviously such programs may occasionally cause difficulty for forensic investigators if it transpires that a case needs a detailed analysis of unallocated space to determine a possible sequence of recent activities.

However, since more than 95 per cent of cases on my records have had no need of such analysis, the loss of deleted material should not cause too many problems. The majority of the remainder involved corporate users where employees had been using company facilities to conduct unauthorised or even downright illegal activity. In such cases, tracing recent activity might be vital to the investigation.

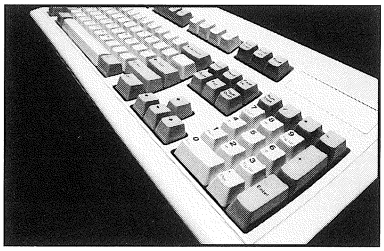
What does concern me is the extraordinary lengths that the software vendors will go to in order to destroy information in the name of security. All of the programs that I have seen will positively erase deleted files.

Most of them will remove deleted filename entries, some will clear slack space and some will even clear the swap file contents. The methods of positive erasure range from a simple overwrite with zeroes through to multiple pattern overwriting of such content and complexity that the oxide coating might fare better being scrubbed with a wirewool pan scourer.

The incidence of computer theft is increasing and it makes sense for individuals to protect their data from prying eyes in the event that the hardware is stolen. But if the data is so valuable, why risk getting it stolen in the first place?

I would have thought that money could be better spent on proper security measures to protect the hardware. Even with space trasher programs, the active file content still remains and a thief is easily going to access it unless some secure password system is in use.

The spectre of computer wizards busily hacking into stolen computers to retrieve priceless information may be useful to sell software but simply doesn't match real life. I have had one case in seven years where deleted material was retrieved and used for criminal purposes and that was on a second hand machine that hadn't been cleared properly.



Is it just my suspicious mind that sees a ready market for such programs amongst the irresponsible users who are aware that their computing activities are illegal and wish to keep them concealed?

Perhaps corporate users might consider this and think about the effect within their internal security departments. The use of space trashers leaves quite clear traces on a machine and if a company had decided to outlaw their use, the mere presence of such traces might itself constitute evidence that there was something to conceal.

For home users, the installation of such "security software" might give them a warm feeling of comfort and safety, but on already overloaded systems is it really worth the effort? These program do have a place - perhaps in certain government or corporate departments on machines carrying extremely sensitive material located in areas where there is an unavoidable risk of theft or illegal access. Otherwise, scrub it!

Jim Bates is president of the Institute of Analysts and Programmers, UK.

Books

30 Minutes to Master the Internet, by Neil Barrett, 64pp, £3

Advertising on the Internet, by Neil Barrett 127pp, £9.99

Kogan Page Limited, 120 Pentonville Road, London N1 9JN

Neil Barrett is infamous in the computer security world as a "poacher turned gamekeeper". He learnt the secrets of the trade from the other side as a hacker, and now uses his acquired knowledge to advise others on how best to protect against such cyber attacks.

In his latest two works he is again discussing the power of the Internet, but this time he is aiming at a domestic and less expert readership.

While these two books are too basic to have much direct relevance to computer forensics, they are nevertheless useful to some degree to police and investigators who are just starting out in the field and need solid information that is easily digested.

The title of 30 Minutes To Master the Internet is a bit of a misnomer, but the book does give a good, if very basic, grounding of the Net. It discusses computers, modems and connection software as well as the various aspects of the Internet such as file downloads, e-mail and newsgroups.

Anyone who can already use the Internet satisfactorily will find little new information in this slim 64-page volume, but for the complete novice it is fine.

Advertising on the Net is interesting reading for anyone who has their own web page. As the Internet develops, it's important for all users to gain the maximum benefit from the wider audience and that means making themselves as high-profile as possible on the Net.

This not only applies to commercial organisations who stand to make money, but also to police forces and government bodies who have web presences so they increase the number of "visitors".

The book covers a reasonably wide area, from links, content and style to "push technology" and web applets. It is written firmly with the non-technical reader in mind, but the downside to this is that it is also lacks absolute detail for those who want to go a step further.

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

Surviving the Year 2000 Problem: Audit's Role

12-13 January 1998
Cumberland Hotel, London
15-16 January 1998

Serzel Plaza Hotel, Stockholm
This briefing is designed for IT and Internal Audit Management.

The briefing will take delegates through the steps which can be taken to help organisations prepare for the millennium change.

Topics will include the legal and professional ramifications of ignoring the year 2000 problem; strategies for gaining corporate support for additional resources; and a methodology for assessing the impact and risks the year 2000 problem will have on organisations.

Delegates will identify the resources and tools available to help their organisations' computers become century compliant.

The briefing leader is Michael T Curtiss, a senior consultant of MIS Training Institute. Previously, Mr Curtiss held technical and management positions with Rockwell International, First Chicago, and Citibank. As world-wide manager for image business development at Unisys Corporation, he was one of the pioneers in the development of image technology.

Contact: MIS Training Institute
Tel: +44 (0)171 779 8944
Fax: +44 (0)171 779 8293
E-mail: drosen@misti.com

International Conference on Forensic Document (ICFD '98)

20-22 January 1998, Bangalore, India

Papers will be presented on the following topics: Identification of Signatures and Handwriting, Obliterations, Erasures, Alterations and Additions, Application of Principles of Pattern Recognition to the Science of Handwriting Identification, Problems and Identification of Printed Matter, Type-scripts and Computer Printouts, Travel and Immigration Documents, Plastic Money and Credit Cards (their use and misuse), Computer Forensics, Age of Documents, with particular reference to ink and paper and bank and insurance frauds.

Contact: Dr R K Tewari, Bureau of Police, Research & Development
Tel: +91 11 436 2676
Fax: +91 11 436 2425

Internet Executive Summit

2-4 February 1998
McLean Hilton, Washington DC, US
Contact: +1 202 973 8693

Corporate Intranet 98 Creating the Networked Digital Enterprise

3-4 February 1998, London

This international conference, which explores the corporate impact and future of web technology, will present Masterclasses on Intranet Implementation and Security Policy, Panel Discussion Sessions, WWW Discussions.

Contact: Business Intelligence Ltd
Tel: +44 (0) 181 879 3399
Fax: +44 (0)181 879 1122

Fraud - Developing a Proactive Role for The Internal Auditor

9-10 February 1998, London
with **Post-conference workshop: Effectively Investigating Computer Fraud and Colating Useful Evidence**
11 February 1998, London

The conference promises a unique opportunity to discover practical techniques and strategies which will focus on the key internal controls and procedures to help delegates successfully combat fraudulent activity.

Sessions include: Creating and Maintaining a Successful Anti-Fraud Culture Within Your Organisation; Examining the Pros and Cons of Fraud Policy Documents; Highlighting the Common (And Not So Common) Early Warning Signs of Fraudulent Activity and Using Them to Effectively to Allocate Your Resources; Identifying Potential Fraudsters at an Early Stage.

The Workshop will be lead by Edward Wilding, senior consultant in the Computer Forensics Department of Network Security Management.

Edward Wilding specialises in computer forensics; computer evidence; the use of intelligence management systems to support investigations into money laundering and intellectual property infringement.

He manages the Computer Forensic Response Team which gathers and analyses computer evidence in civil and criminal cases.

Programme topics are: Legal Considerations, Identifying the Issues Associated With High-tech Computer Fraud and Abuse; Scene of the Crime: Getting to Grips With the Procedures Which Must be Initiated Immediately; Understanding the Intricacies of Computer Back-Up Methods; Evaluating the Need For Covert Investigations; Identifying the Key Considerations of the Main Corporate Operating System and Abuse and Misuse Associated with the Internet, Mainframe, Minicomputer and Network.

Contact: IIR Ltd
Tel: +44 (0)171 915 5182
Fax: +44 (0)171 393 0313

IT Auditing and Controls: Integrating the Auditor

9-10 February 1998, London

Auditing Automated Business Applications

11-13 February 1998, London
Contact: MIS Training Institute
Tel: +44 (0)171 779 8944
Fax: +44 (0)171 779 8293

Integrated Communications 98 and Smartcard 98

17-19 February
Olympia 2, London
Contact: +44 (0)1895 454438

Internet World UK exhibition

May 12-14
Olympia 2, London
Contact: +1 (0)1865 388000

International Journal of FORENSIC COMPUTING™

Published by
Computer Forensic Services Ltd