The threat of computer crime: identifying the problem and formulating a response at force level.

Andy Bliss
Sussex Police

Clive Harfield
University of Wollongong, clive@uow.edu.au
The threat of computer crime: identifying the problem and formulating a response at force level.

Abstract
Computers impact on many aspects of daily life and increasingly are utilized in a wide range of criminal activities. They facilitate actions which might come to be considered criminal but which, as yet, are not illegal and they have affected the nature of victimization. Inevitably police forces are having to come to terms with this new phenomenon. This article presents research undertaken by Sussex Police in identifying the extent of the potential problem (elsewhere previous studies have focused on the nature of the problem) and in formulating a response. The work was undertaken by a Computer Crime Working Group of 15 officers and specialist support staff, including the present authors. The Group's Report was submitted to the Sussex Police Crime Management Sub-Committee in December 1996.

Keywords
formulating, response, force, level, identifying, crime, computer, problem, threat

Disciplines
Arts and Humanities | Law

Publication Details

This journal article is available at Research Online: http://ro.uow.edu.au/lhapapers/1597
THE THREAT OF COMPUTER CRIME: IDENTIFYING THE PROBLEM AND FORMULATING A RESPONSE AT FORCE LEVEL

Computers impact on many aspects of daily life and increasingly are utilized in a wide range of criminal activities. They facilitate actions which might come to be considered criminal but which, as yet, are not illegal and they have affected the nature of victimization. Inevitably police forces are having to come to terms with this new phenomenon. This article presents research undertaken by Sussex Police in identifying the extent of the potential problem (elsewhere previous studies have focused on the nature of the problem) and in formulating a response. The work was undertaken by a Computer Crime Working Group of 15 officers and specialist support staff, including the present authors. The Group's Report was submitted to the Sussex Police Crime Management Sub-Committee in December 1996.

The Crimes and the Victims
Criminal use of computers is limited only by the imagination: they can forge both paper and electronic documents; drugs dealers use them; paedophiles exchange pornography via the Internet; companies are defrauded by employees misusing computers at work; accounts can be altered; billing systems disrupted; software is pirated. Hacking is used either to obtain unauthorized access to secret or commercially sensitive information, or to commit electronic criminal damage by injecting into computer systems viruses and other types of software programs intended to disrupt and damage software and data. This latter crime can range from a level equivalent to teenagers spraying graffiti over a bus-stop to political activists and terrorists systematically destroying the information systems of companies and government agencies. Unauthorized access to and disclosure of personal or company information can lead to threats such as blackmail, and to manipulation of the free market to obtain unfair advantages over rival companies.

The victims are not only corporate. Individual citizens can fall prey to unlawful disclosure of information or electronic theft. Children are victims of computer pornography, and computer crime can result in
secondary victimization where a company is put out of business and both its employees and its clients suffer the consequences of redundancy and threats to their own business. The collapse of a major employer in a relatively small community will impact on the local economic infrastructure. Individual victims tend to excite more agitation for law and order and more sympathy than corporate victims, yet the threat to society of corporate crime may have far-reaching consequences. Computers significantly alter social and economic interaction on a wide scale. With new electronic relationships come new possibilities for crime.

The Computer Crime Scene

With modems, mobile phones and lap-top computers, crimes can be committed anywhere, anytime. The concept of a crime scene is radically redefined because a computer and a telephone in one country can be used to commit crime electronically in another ('Superhighway Robbery', Channel Four TV, December 8, 1996). Not only has the potential scale of the scene increased from, say, a single room or dark alleyway to the entire world, but also the nature of the evidence at the scene has fundamentally changed. It is electronically formed, invisible and intangible. Traditional scene investigation methods are not applicable to this type of evidence. New techniques are required to recover the evidence, and to present it comprehensibly at court. Rather like the archaeologist excavating the past, the investigator of computer crime alters and destroys the evidence as soon as active investigation of the hard-drive commences. Unimpeachable evidence audit trails will be vital to successful prosecution.

Will victims consent to such evidence being used by the police? Anderson (1995) notes that banks consider their security systems fool-proof and deny the possibility of false withdrawals from cash dispensers. In effect banks accuse their customers of fraud in such circumstances, by inference if not in actuality. Police investigation into such allegations is hampered when a bank refuses to allow interrogation of its computer systems and as a consequence the evidence cannot be tested in court. Yet the rules of evidence require that the breach of security systems be proved in order to demonstrate fraud has taken place instead of machine malfunction.

Still in its infancy, the science of computer forensic examination is resource intensive. Expertise is relatively rare and consequently expensive. Force consultancy budgets are already stretched. The demand for computer investigation will only increase. For the entrepreneur the potential exists to set up private computer investigation companies. This may be an alternative to the provision of public police services for the investigation of this type of crime because of the resources involved, but computers are used in such a variety of crimes that if the Police Service does not confront this use there is a danger of the service disqualifying itself from the investigation of a significant
amount of crime. Criminal use of computers affects not only the nature of crime, but also the nature of policing.

**Legislative Tools**
The Computer Misuse Act 1990 was the first UK legislation targeted specifically against the phenomenon of computer crime. Failed prosecutions suggest that this legislation is not as useful as it might be (Collier and Spaul, 1992: 319). The House of Lords has recently questioned whether certain actions hitherto perceived to be deception are crimes at all if a computer is used (R. v. Predy, Slade and Dhillon (1996) 3 All ER 481; Police Review, December 6, 1996, pp.16-7). This has prompted an urgent review of existing legislation. As technology out-stripped existing social conventions and prohibitions, the crime of abstracting electricity had to be enacted to cover behaviour not addressed by the then current theft law. Legislation now has to catch up with computer technology.

The whole area of computer crime law is vast, complex and beyond the scope of this paper. Two papers summarize the issues. The comprehensive Report on Computer-Related Crime by the Council of Europe (European Committee on Crime Problems, 1990) highlights the universal nature of the threat. "In all of the industrialized states, the same phenomena of computer crime have appeared; prosecuting authorities almost everywhere have to contend with similar difficulties in the application of the traditional domestic criminal law to this new form of crime; dramatic cross-border cases demonstrate the increased need for international cooperation" (ibid., 20). Computerization has led to new types of personal and property interests which have to be protected, although not necessarily by the criminal law. The Council of Europe called for uniformity in legislation on computers between member states. This pan-European perspective contrasts with Clark (1994) who focuses on how Eire has approached the problems of computer crime. He makes a number of contrasts between the Irish and British legislation. These two papers demonstrate the nature of the debate. Discussion focuses on what behaviour should be criminalized, how legislation should be drafted, and how evidence should be gathered and presented. Examples of crimes committed are cited which demonstrate the international aspect of computer crime, the commonality of behaviour, and the fact that not all actions are universally criminal.

Within English legislation, ss.19(4) and 20(1) of the Police and Criminal Evidence Act [PACE] deal with some aspects of the retrieval of electronically-stored evidence. The Law Commission Report on Computer Misuse (No.186, Cm 819, 1989), around which the Computer Misuse Act 1990 is drafted, did not consider whether the existing rules of evidence would enable successful prosecutions under the Act (Doran, 1990: 379). This omission means that trials within trials may have to resolve the admissibility of computer evidence. Some evidence will
only be accessible if telephones are intercepted and the free consent of victims to have their end of the telephone line tapped may be an alternative to obtaining warrants, but the police will need to demonstrate that they themselves are not committing the offence of unauthorized access when gathering evidence. Sections 69 and 78 of PACE may decide the future role of computer evidence and whether or not, under current legislation, computer crime can be properly policed (ibid.). Meanwhile Corbitt (1996) discusses what can be done with current legislation and considers the points to prove.

The Strategic Threats to Police Forces
The above discussion provides a context within which to consider the threat of computer crime at force level. Clearly many of the issues are of a national, legislative nature and so are not within the sole remit of the police service to resolve. The police have to respond to the current demands, and they have only current legislation to rely on.

There exist a number of strategic threats to police forces posed by computer crime. Increasingly reliant on computers, police forces themselves are potentially as vulnerable to computer crime as any organization. Strategic planning must take account of this, together with the likely future policing demands resulting from increased criminality and increased awareness of computer crime among operational officers. Where computers are both tools to commit crime and targets of crime, the increased use and illegal acquisition of information technology by criminals will impact upon the crime rate in a force area. Correct preservation and handling of evidence is essential to maintain detection rates in line with performance targets and the particular difficulties presented by computer crime in relation to this have already been alluded to. Incorrect police interrogation of suspected computer evidence may lead to the unwitting destruction of innocent yet commercially valuable material and render a police force liable to civil litigation and claims for damages. Where the loss of commercial information leads to business bankruptcy and the loss of jobs, civil liability may well run to millions of pounds. The Association of British Insurers currently estimate that claims resulting from stolen hardware and subsequent data loss total £200M a year (University of Manchester/GMP 1996: 23). The use and disclosure of inaccurate information held in police intelligence systems, acts by definition unauthorized (Data Protection Act 1984), has already resulted in some forces having to pay damages.

Identifying the Threat in Sussex
Collier and Spaul note the dearth of reliable statistics about the extent of computer crime (1992: 308-311). There are no police statistics, and commercial organizations are understandably coy about admitting their vulnerability. Only 10% of those private companies surveyed responded to the 1994 Audit Commission survey, compared with 51% of public
sector organizations contacted (Audit Commission 1994: 8). Fifty % of all computer fraud is discovered by chance (Audit Commission 1994: 11). There is little likelihood of offenders being caught or even of crimes being reported. The British Crime Survey does not include questions about individual victims of computerized crime.

Other than Guinney's research into computer awareness among detectives (1992) there were no models available with which to assess the possible threat in the Sussex Police area. In the absence of other research about the extent of computer crime it was necessary to undertake original research within Sussex; a police area comprising the two counties of East and West Sussex, with a population of roughly 1.4 million.

The Sussex Police Computer Crime Working Group was set up in July 1996 and was tasked to report by December 1996. It was decided to survey operational sergeants and constables about their experiences of encountering the criminal use of computers. Previous studies, such as that of the Audit Commission (1994), have focused on the victims and have relied on self-reporting. Reluctance to report means that such surveys never reveal the extent of the problem. The encounters experienced by operational officers will include those crimes in which there are no reporting victims, such as drug-trafficking, as well as such victim-generated reports as are received. It was also anticipated that the survey would identify practical problems faced by operational officers, again something a victim-survey would not achieve. This survey was intended to be one of the contributions to a three-part report examining the potential threat, the most suitable response and the implication of evidence recovery and legal issues.

Survey methodology in social science is well attested (Hibberd and Bennett, 1990; Hagan, 1993: 128-54) and guided this research. A confidential self-completion questionnaire survey, designed by the second author and validated by the Sussex Police Survey Analyst, was conducted between September 2 and September 30, 1996. Participation was not compulsory -167 questionnaires were sent out to both uniform and detective operational sergeants and constables across a range of disciplines (general uniform patrol, specialist squads etc.). The randomly selected sample represents 7.2% of Sussex Police operational strength; 126 responses were received equating to a response rate of 75.4%, higher than had been expected. Respondents were asked about their encounters with computers in a criminal context over the 12 months immediately preceding the survey.

The full report on the survey is an internal Sussex Police document; some of the 'head-lines' present a picture of the threat of computer crime in one provincial force area. Other forces may find these results instructive.

• 39% of those surveyed had been the first officer on the scene of a burglary or theft where a computer, parts of a computer, computer

January 1998  The Police Journal  29
disks or an electronic organizer had been stolen.

- 26.8% of those surveyed had been investigating OICs in cases where evidence relevant to the crime was stored electronically on a computer.
- 56.1% of those surveyed had encountered a computer, parts of a computer, computer disks or an electronic organizer when conducting a search under warrant or PACE powers.
- 36.5% of respondents had seized as evidence a computer, parts of a computer, computer disks or an electronic organizer during the 12 months prior to the survey.
- 74% of OICs sought expert advice when recovering evidence stored on a computer, computer disks or an electronic organizer.
- 24% of OICs tried to interrogate a computer or an electronic organizer for evidence themselves or else sought the help of a colleague who "knew a bit about computers".
- 16.6% of respondents had used their powers under s.19(4) and s.20(1) PACE to seize evidence stored in a computer in a visible and legible form. At least one respondent had required the suspect to do this.
- 20.6% of respondents were unaware of the above powers.
- 49.6% of those surveyed owned their own computers or electronic organizers, or both, but no correlation between personal ownership and recovery during searches or personal attempts at retrieval was evident. The level of personal ownership may be a guide to general awareness within the organization, but it does not reflect level of expertise or ability in evidence recognition and retrieval.

Computers were most often encountered in connection with drugs-related crime, although more individual officers had encountered computers being used to store or send obscene photographs. Nine respondents had each encountered the use of computers in drugs-related crime on five occasions or more in the previous 12 months. Of these nine, one was on the drugs squad, three were uniform patrol officers, four were CID officers and one was a Special Branch officer. Thirty respondents had encountered more than one type of crime in which computers were being used.

Extrapolations based on a sample survey population must be treated with some caution. Nevertheless on the basis of reported encounters the survey findings suggest that across the Sussex Police area evidence electronically stored on a computer may be encountered up to 11 times each day, a higher frequency than had been anticipated.

**Formulating a Response**

There were a number of lessons to be learnt quickly. The survey itself increased awareness of computer crime among operational officers. Before the survey the scientific support manager was receiving one or two inquiries a week about the possible forensic examination of computers. These inquiries came daily after the survey. Clearly the
recovery of evidence from computers is a real issue. Guinney (1992: 13) cites an example of why there has to be increased awareness. A paedophile in Hampshire computerized all his records of contacts, customers and girls because he gambled that any police officers searching his premises would only seize paper documents. He was right. Incriminating evidence and considerable intelligence stored on his computer was not seized because searching officers ignored his computer. Other forces who survey their own staff should be prepared for the increased awareness which will result simply from undertaking such a survey.

Secondly there was a need to determine just when scarce resources should be allocated to a full forensic interrogation of computer evidence. It may not be necessary for a full forensic examination of electronically-stored evidence to be carried out in each case that evidence is expected to be found stored on a computer. Operational officers need clear guidance on this matter and indeed over 40% of those who responded with volunteered free text answers to the ‘any other comments’ survey question specifically requested such guidance. The ubiquitous aide mémorable card is one possible solution.

Thirdly there was a clear training need on procedures to adopt when seizing computers. The ACPO Crime Committee has published some advice on this (ACPO 1996: 29-31). Officers may need reminding of their PACE powers although who actually produces the visible and legible form of electronically-stored data remains an issue. A suspect can be asked to do it, but there exists the risk that he or she will alter or destroy the evidence instead. Any officer trying to do it will need to know exactly what he or she is doing, and will need to be able to account for every step in court at a later date. Officers need to be advised about the use of anti-static bags in which to seal computer parts. They also need the anti-static bags. Here there is a danger of over-familiarity. All officers in Sussex Police have access to the force operational and intelligence systems on computer. Familiarity with a key-board and VDU does not mean officers will recognize a dismantled computer and its constituent parts. The City of London Police and Thames Valley Police both publish booklets with photographs of computer parts; also the tools needed to remove such items so that criminals going equipped to steal can be identified by police officers. Elsewhere posters and videos are available on a similar theme.

Nor will the daily use of a computer in the police station equip officers with the skills necessary to undertake their own interrogation of the software and hard drives. That one in four officers in Sussex has apparently tried to retrieve electronically-stored evidence for him- or herself is a matter for concern if these officers are not fully expert in the operations of all computers. Clearly many computers examined will have contained no evidence but any person presenting computerized evidence from the witness box must expect to have to deal with rigorous cross-examination from defence lawyers. There must be a reasonable
prospect of conviction for a prosecution to proceed. The evidence must also be capable of withstanding cross-examination. A do-it-yourself retrieval of computerized evidence is likely to fail both these tests.

It is reasonable to expect that if similar surveys were conducted in other forces, the results would not be so very different. The guiding principle is the need to maintain a sense of perspective. Not every computer encountered will need to be seized. Not all seized computers will need the sort of full forensic examination currently undertaken at great expense by various companies and consultants. A lower level of interrogation may be suitable in a number of cases, and it should be possible to train officers to operate on-site copying equipment (where the contents of the hard drive are copied without removing the computer) with knowledge of the basic procedures in the same way that officers are trained in the use of Intoximeter machines in order to satisfy a court that they are familiar with its workings. Providing such officers know how to operate a machine competently there will be no need for them to be trained to the level of theoretical computer scientists.

When an attempt was made to measure how much computer hardware was being stolen, and what sort of equipment was attracting thieves, problems were encountered because of the huge variety of ways in which computers and computer parts are described by owners, and by police officers on crime reports. In view of this a simple explanation of the different parts of a computer for officers to use on crime reports may assist in the later analysis of crime patterns. Expert opinion is divided on the issue of computer theft. Some believe that the current vogue for memory chips will pass just as the wide-spread accessibility of video recorders led eventually to a decrease in the numbers being stolen. Others argue that as new generations of computers are produced, each requiring more memory, memory chips will always retain their value as a criminal currency. Consequently, sites containing a large number of computer processing units will remain targets for thieves stealing to order. The next generation of computers is due in early 1997.

Crime prevention advice should not confine itself to target-hardening advice offered to those likely to be burgled. Organizations need to be able to access advice on how to prevent the misuse of their computers as well. It often transpires, if such crimes are ever discovered, that a trusted employee is responsible for fraud costing his or her company tens of thousands of pounds, and sometimes hundreds of thousands (Audit Commission 1994: 21). Responsibility for effective supervision and auditing lies with the organizations who use computers. Sound management practices will form part of the auditing trail for prosecution evidence, and this message needs to be put across if the police are to tackle these sorts of crimes.

**Conclusion**

Computer crime is an emerging criminal phenomenon. Many lessons are yet to be learnt. New legislation will be required as new behaviours
are deemed socially unacceptable and existing laws are found to be inadequate to deal with the problem. Issues of international jurisdiction will have to be considered at inter-governmental level. The nature of the problem has been much publicized and discussed. The extent of the problem is less certain, and it is in this area that this article has sought to make a contribution.

The research conducted in Sussex has demonstrated the likely scope of the threat, and this has enabled an informed response to be implemented. The research could form a model for other forces to adopt when considering their own policies. The problem cannot be ignored and as more crimes come to notice, this will impact upon force performance, resource allocation, and the service offered to the public. At individual force level there needs to be an awareness of both the nature and the extent of the problem and strategic planning for a response policy which will maximize evidence and intelligence recovery within the constraints of limited resources.

The police are not necessarily the only agency that can be employed in the fight against computer crime. The DTI and the Serious Fraud Office both employ multi-disciplinary teams to police their jurisdictions. Customs and Excise are also involved in the investigation of drug-trafficking offences and encounter the considerable use of computers. The police service needs to determine its position within the overall investigation of computer crime. Whilst not suitable for delegation to another agency (in the manner that the SFO now deal with major fraud), the police are unlikely to have sufficient resources to deal with the whole problem themselves. In the area of fraud the Police Service allowed itself to be marginalized as fraud became ever more complex and international in nature. Computer crime will inevitably become so inextricably woven into the fabric of criminality that this is one aspect of crime the Police Service must address.

Acknowledgements
The members of the Sussex Police Computer Crime Working Group, whose research has contributed both indirectly and directly to this article are: Neil Cuttress, Ken Duerden, John Fielding, Martin Gaule, Adam Hibbert, Dave Leeney, Roger Linthwaite, Andy Luczkowski, Vic Marshall, Eddie Redman, Peter Savage, Brian Underhill, and Liz Walker.

The views expressed in this article are those of the authors alone.

Bibliography
University of Manchester (Henry Fielding Centre) and Greater Manchester Police (1996) A Growth Industry: The Proceedings of the First National Conference to Address the Theft of Computer Hardware and Component Parts, University of Manchester.

* * * * *

NORTHUMBRIA HOUSEHOLDERS HELP POLICE
Householders in Northumberland and Tyne and Wear were asked to take part in a large public consultation exercise to find out which crimes local people are most concerned about and which ones they think local police officers should be targeting. Over half a million leaflets were distributed inviting the recipients to give views by filling in a tear-off form with their comments and posting them free of charge to the police authority. The leaflet also contained details of FreeCall telephone lines and a Minicom line where members of the public could pass on their comments trained operators. Northumbria Police aim to draw up a Policing Plan in the light of the consultation which will help to direct resources to where they are most needed. The plan will be published in the spring of 1998.

PUBLIC SERVICES LISTENING TO THE PUBLIC
Hertfordshire’s two health authorities, the county council and police authority are joining forces in an initiative to communicate better with the people of the county. A panel of more than 2,300 residents has been set up to act as a sounding board for the authorities’ policies over the next three years. Including people from all areas of Hertfordshire, of all ages and from all walks of life, the panel have agreed to take part in regular postal questionnaires and occasional discussion groups. Following a tender exercise, the authorities have selected the market research company MORI to run the poll on their behalf. The Associate Director of MORI commented: “At a time when resources are so tight, it is even more vital that agencies are getting solid feedback on how they are doing. By working together, they are maximizing their value for money and making it possible to look for the county as a whole, rather than only for their own organization.

PARTNERSHIP CAMPAIGN TO FIGHT DRUGS MISUSE
The Metropolitan Police Service joined forces with Blockbuster Entertainment and the Health Education Authority in a nationwide drugs awareness campaign. The month-long campaign in the autumn of last year aimed to make information on the effects of drugs more readily available to parents and young people across the UK. As part of the campaign, the Met’s award-winning drugs video resource pack A Pack of Truths was trailed in all of Blockbuster’s 730 stores and in-store publications.