Artificial Intelligence Review **6**, 203—215, 1992.

A forensic methodology for countering computer crime

P. A. COLLIER and B. J. SPAUL

Computer Crime Research Group, University of Exeter, Exeter, Devon, U.K.

Abstract. This paper argues that the moves by police and consultancy firms to successfully enforce recent computer misuse legislation requires the bringing together of investigative, legal, courtroom and computing skills in an extension of forensic science. The term suggested for this new discipline is computer forensics'.

Key Words: Computer crime, Forensics

1. INTRODUCTION

According to a Council of Europe Committee of Ministers report (1989) "computer-related crime is a real and, at least in respect of certain offences, expanding phenomenon." The impact of computer abuse is illustrated by a recent report carried out by the London Business School (reported in *Management Accounting*, March 1990), which put British annual losses from computer fraud at over £407 million. The survey supports the findings of other UK surveys like the Audit Commission (1987), which reported an increase in both the number of incidents and losses and observed that "opportunities for misuse continue to increase in line with technological advance." These results together with similar reports from the US (for example Hoffer and Straub 1989) suggest that computer crime is a threat, which it would be unwise for businesses to ignore. Such findings, plus increased publicity on hackers and viruses (see for example Bowcott and Hamilton 1990), gave rise to business pressure for legislation, which led to the passing of the Computer Misuse Act in 1990.

This legislation may not solve the problem. As Stanley (1986) stated there are the major problems in investigating computer crime:

(i) competency of the investigators;
(ii) definition/terminology difficulties;
(iii) evidentary problems; and
(iv) jurisdiction/law deficiencies.

and legislation only deals with the last of these. This statement is supported by recent history on the success of the authorities in prosecuting computer crime. For example, the latest Department of Trade and Industry figures, as reported in PC Business World 13 February 1990, reveal that of 270 computer crimes notified in the last five years only six have been prosecuted. This problem is not confined to the UK, in Germany in 1987 2777 cases classified by the police as computer crimes resulted in only 170 convictions and in France, since the

passing of their computer misuse legislation, only 10 of the 70 substantiated complaints to the police have been successfully prosecuted in the courts (Council of Europe Committee of Ministers report 1989).

Any system of controls can be classified as either proactive or reactive. In relation to computer crime proactive controls are responsible for preventing criminal acts by reducing opportunities, this type of control is emphasised in computing and accounting literature. However, these controls alone have proved insufficient to stop the increase in computer misuse and reactive controls, such as the effective detection and prosecution of computer criminals, must supplement them. This paper discusses how the laws against computer crime can be enforced. A crucial element in achieving this will be the development of a forensic methodology for application to computer crimes and abuses.

2. DEFINITION OF FORENSICS

The word forensic is defined in the Oxford English Dictionary as an adjective meaning ". . . used in, or connected with a court of law." and the term forensic science as "a science that deals with the relation and application of scientific facts to legal problems." Traditionally forensic science has centred on the physical and applied sciences such as medicine, engineering, chemistry, ballistics, etc. However, more recently social sciences, such as psychology and accounting, have been added to the forensic science armoury. These social science extensions of forensic science have a dominant requirement for interpretive and judgemental skills, rather than the detection of physical evidence. This paper advocates an extension of forensic science to cover crimes committed using computers. The extension is termed computer forensics and would cover the collection of forensic evidence from computers for use in a court of law. This requirement establishes a standard of work for the forensic systems analyst or investigator. Public scrutiny in a court of law places unique burdens on forensic scientists. For the computer forensic expert the problems are exacerbated by the obvious difficulties of explaining the complexity of criminal computer based activities to a jury of twelve members of the public, and uncertainties in the UK on what constitutes admissible computer generated evidence (see for example Walden 1989).

3. ROLE OF COMPUTER FORENSICS

Computer forensics is new in that it gives a label to existing but very limited activities amongst the police and consultancy firms. The different areas in which computer forensics could play a constructive role include:

(i) Civil matters — there is an increasing need for expertise in the investigation and assessment of the integrity of computer systems in civil cases. The estimation of the size and nature of losses from negligence, invasions of

privacy, industrial espionage and social nuisance (e.g. the release of viruses) are increasingly required in civil cases.

(ii) Criminal matters — recently white collar crime has become increasingly computerised as criminals recognise the potential for crime given by the anonimity of computer systems and the development of electronic funds transfer systems and electronic data interchange systems.

(iii) Insurance — the preparation and assessment of insurance claims arising as a result of system failure or penetration, on behalf of both insurers and the insured may well require the assistance of a forensic systems analyst.

(iv) Government — the forensic systems analyst can assist governments with regulatory compliance by ensuring that the appropriate legislation is being applied in private organisations, where applicable.

4. REACTIONS TO THE THREAT OF COMPUTER MISUSE

As has been stated, firms have a vested interest in improving proactive controls and making computer crimes harder to commit. Senior management must accept that computer crime poses a real threat and impose cost effective measures for its prevention. The exact controls used vary between organisations but a strengthening of personnel procedures, physical access restrictions, tightened password procedures, better supervision of computer staff and securing data transmissions are typical defensive measures.

Some governments reacted to computer misuse by focusing on detection, prosecution and deterrent sentences. The UK has belatedly, in comparison to the US, Canada and much of Europe (Hollinger and Lanza-Kaduce 1988), recognised computer crime as a separate offence. The growth in computer crime also requires that society ensures that those who are prevent, detect or otherwise counter computer crime are properly trained. This need has been recognised in the Netherlands (*Computer Weekly*, 25 October 1990) where the Dutch police have established an experimental squad of specialised computer crime detectives at a cost of some £5 million to improve conviction rates. At a minimum training should cover:

(i) the police — according to Cornwall (1988) out of 144,000 police officers only four or five officers concentrate on computer crime at any one time. A unacceptable situation given the importance of securing evidence as soon as a crime is detected.

(ii) the Crown Prosecution Service — prosecuting barristers specialising in computer crime are essential if the current prosecution success rate is to be improved.

(iii) Senior management in public and private sector organisations — countering computer fraud requires that management in all organisations be aware of the threat and the importance of a systematic approach to it's prevention, detection and prosecution.

(iv) Security officers in public and private sector organisations. Despite coun-

termeasures, computer crimes will occur in firms an important deterrent is the 'on the spot' expert.

5. THE COMPUTER FORENSIC METHODOLOGY

Currently assistance with prosecuting crimes which involve computers is available from two sources: consultants; and the police. The appropriate agency to give assistance will depend on the investigation process, which can be viewed from two standpoints:

(i) internal investigations — carried out by the possible victim organisation or their agents, perhaps as a preliminary to involving public agencies, or until sufficient evidence is collected to pursue a civil case.
(ii) external police investigations — either from the outset, utilising a specialist team of experts, who deliberately distance themselves from employees of the victim organisation, or following on from an internal investigation.

The skills implicit in a computer forensic approach to a computer crime investigation will probably be provided by a multi-disciplinary team of a similar constitution regardless of whether an internal or external investigation is taking place. However the modus operandi of the two types of team would necessarily be quite different.

The members of a forensic team conducting an investigation will have the following skills:

(i) investigative — to supervise the conduct of the investigation and interview suspects and witnesses;
(ii) legal — a knowledge of the laws which can be applied against computer related offences and the laws of evidence;
(iii) court room presentation — acting as a witness or expert witness; and
(iv) computing — to uncover how the crime was committed, assist in reconstructing computer evidence and tracing proceeds of the crime.

Although computer forensic skills are currently provided by those with police, legal and computing skills; if the growth of computer crime continues, it is possible that computer forensics specialists with the complete range of skills listed above will emerge from consultancy firms or be provided by the police.

Having outlined the areas of expertise it would be useful to examine each of the skill areas identified in greater detail.

6. INVESTIGATIVE SKILLS

Computer forensics skills should include the conduct an investigation into computer crime or abuse. Nasuti (1986) suggested that computer crime investigations should be based around a formal action plan prepared for this eventuality. In particular the plan should cover:

(i) objectives — guidelines on defining the scope of the inquiry. Management must specify the goals, which could include recovery of past losses,

discovering how the crime was committed, identifying controls to prevent a recurrence but not prosecuting the perpetrator, identifying the perpetrator and collecting sufficient evidence to support a dismissal or identifying the perpetrator and pressing criminal charges.

(ii) notification — standard internal procedures should exist for notifying senior management and relevant outside bodies. The maintenance of secrecy is important in computer crime cases as computers facilitate either the destruction of evidence or malicious damage to the installation by the alerted perpetrator. At a minimum those notified should include the board of directors, the heads of internal audit, finance and

(iii) membership of an investigating team.

Computer forensic skills will be involved in deciding upon an action plan irrespective of whether the investigation is internal or involves the police. The likely major steps to be followed include:

(a) determine the exact nature of the computer crime or abuse and whether it is ongoing or complete;

(b) identify how the crime was committed and the hardware and software involved;

(c) determine whether the crime was a solo effort or relied upon collusion and whether the perpetrator(s) came from within or from outside the organisation;

(d) determine sources of evidence and their admissability;

(e) identify possible witnesses and suspects;

(f) examine personnel records of suspects for 'red flag' indicators (Albrecht *et al.* 1984) such as not taking holidays, a possible grudge against the organisation, extravagant lifestyle and falsified references.

(g) interview witnesses and suspects; and

(h) analyse and reanalyse the evidence gathered on a continuing basis.

As well as skills in managing the investigation, computer forensics requires the ability to interview suspects, analyse evidence and quantify losses. Although managers may have the skills to interview job applicants or counsel staff, interviews in the course of a computer crime investigation will require special abilities and may well best be left to the police. The following general guidelines apply:

(i) the interview should be carried out by two or three people (more would intimidate the interviewee), notes should be taken and the interview tape recorded. At the end of the interview the tape should be copied and handed over to the company solicitors or police in return for a timed and dated receipt to remove accusations of the recording having been tampered with.

(ii) The objective of the interview is to, as stated by Comer (1985), 'create such empathy and confidence that admissions and confessions are almost obligatory'. Achieving this requires a three stage approach. The first stage involves building empathy and demonstrating that the truth will inevitably out. Following this the interviewer builds up the stress by showing that the interviewee will inevitably be found guilty and that therefore a confession

is the only sensible option. Once guilt is admitted the interviewer in the final stage obtains detail of the crime.

Investigative skills also require an ability to analyse and reevaluate evidence collected and the results of interviews. In essence, the process is akin to solving a puzzle with the important difference that it may never be solved. At the least the method of the crime must be determined so that controls can be strengthened. Finally investigative skills cover the documentation of the investigation in a form suitable for management and perhaps the prosecuting authorities.

Finally the investigative team will need to quantify the losses, both direct and consequential, consider the wider financial implications of the matters under investigation and instigate procedures to trace monies lost.

7. LEGAL SKILLS

Until August 1990 and the Computer Misuse Act, there was no such thing in the UK as a computer crime (except the Data Protection Act 1984) and therefore the prosecution of offences involving computers had to be based on existing statutory offences. The Act has simplified the position and criminalised the following three actions:

(i) unauthorised access to computer material (section 1)
(ii) unauthorised access with the intent to commit or facilitate the commission of further offences (section 2)
(iii) unauthorised modification of computer material (section 3)

To prove that an offence has been committed the following must be demonstrated:

(a) the computer performed a function as a consequence of access being attempted or actual access (sections 1 and 2);
(b) the access was unauthorised (sections 1 and 2);
(c) the person attempting access knew that it was unauthorised (sections 1 and 2);
(d) the access was a preliminary to committing or facilitating a serious offence (section 2);
(e) the modification to computer material was or would have been caused (section 3);
(f) the modification was unauthorised (section 3);
(g) the person attempting the modification knew it was unauthorised (section 3); and
(h) the intention of the modification was to impair the computer's operation (section 3);

It is no easy matter to establish these points. At a minimum there must be an access control system with a secure log, which records all accesses, but even then it is necessary to link the terminal being used with the perpetrator of the offence. This would only be easy if a person authorised to certain access attempted to exceed these limits while signed on under his own password.

Otherwise the person using the terminal would need to be caught in the act. Even in the first situation the user could throw doubt on the evidence on the ground that the user:

(a) left the machine logged on and the unauthorised access was by a third party taking advantage of the situation; or
(b) was the victim of a compromised password.

The demonstration of intent in the section 2 offence may be even more problematic. In the event of hacking, the multiple password attempts recorded in the access control log will provide some evidence but further evidence will probably depend on the nature of the system being accessed. The proof of unauthorised modification is straightforward provided that there are regular back ups, secure transaction logs and clear rules on the types of transactions employees are authorised to carry out.

The Act has simplified the prosecution of persons responsible for attempting to or actually penetrating a computer system and those introducing viruses or other rogue software. The offence is punishable by a fine and/or term of imprisonment.

The Act belatedly brings English law into line with the situation in the US, Canada and much of Europe. For example, in the US virtually all states (excepting District of Columbia, Maine, Vermont and West Virginia) have followed the lead of Florida and Arizona in 1978 (Tapper 1990) and have enacted specific laws against computer abuse often following a model computer law available from the Data Processing Management Association. In 1984 and 1986 Congress enacted two pieces of computer crime legislation (US Public Laws 98—473 and 99—474) and in January 1988 state laws were strengthened by a federal Computer Crime Act. Similarly in Canada, the Criminal Code Section 301.2 states that a mischief is committed by persons who wilfully: destroy or alter data; render data meaningless, useless or ineffective; obstruct, interrupt or interfere with any person in the lawful use of data; or denies access to data to any person who is entitled to access thereto. In France, Article 462—2 of the Law 88—19 provides an offence of fraudulent access to a machine, West German legislation made it illegal to gain unauthorised access to secure computers and the Swedish Data Act 1973 is probably the earliest creation of the offence of gaining unauthorised access to a computer. Currently, according to the Law Commission (1989) only Belgium and Japan of major industrial rely upon existing laws to counter compute crime and abuse. The Computer Misuse Act 1990 also covers the Law Commission's recommendation (Law Commission report number 180 1989) for surmounting the jurisdiction problem, which arises in situations such as where a terminal in New York can be used to access computers in the UK, by merely requiring in clause 4 that must be at least one significant link with the domestic jurisdiction for the legislation to apply.

Currently relevant offences, which extend and might be use in conjunction with the Computer Misuse Act 1990, in the context of computer forensics are:

(i) Theft Act 1968 s.1(1) and s.17(1), which define the offense of false accounting as the alteration, concealment, destruction or falsifying of accounts. However the Act would not cover the theft of information since

as Lord Upjohn observed in Boardmann *v* Phipps "In general, information is not property at all" — therefore it cannot be stolen. This prevents prosecution under the act in datatheft situations where access is made to computer files purely to obtain information.

(ii) Theft Act 1968 s.15(4) which covers deception. Its applicability to computer crime is limited in that it is the human mind (and not the computer), which must be deceived.

(iii) Forgery and Counterfeiting Act 1981, which is relevant in situations where a person makes a false instrument with the intention that it shall be used to induce somebody to accept it as genuine. In R *v* Gold and Schifreen (1988), the Act's applicability to computer crime was reduced by the requirement that something of permanence must come into existence. However, it may be relevant where access to the computer is obtained via a forged device, for example a fake electronic identity device, or possibly if the computer were manipulated to raise documentation which authorised the movement of goods or money. However, it is probable that the alteration of data within a computer, which subsequently leads to documents being issued which cause a deception, would not be covered as the computer and not the person has been deceived and made the false instrument. In probability the use of this Act will be unnecessary given the new misuse legislation.

(iv) Criminal Damage Act 1971 s.l(1), which covers the unlawful destruction or damage of another's property or reckless behaviour leading to leading such damage or destruction, is suitable for prosecuting malicious acts against the computer and files and topical computer abuses like viruses trojan horses and logic bombs as described in Burger (1988). This act was use in Cox *v* Riley (1986) when the defendant deliberately erased a computer program from a plastic circuit card of a computerised saw so as to make it inoperable and again in May 1990 R *v* Whiteley resulted in the successfully prosecution in the Crown Court of virus attacks on university computers. Notwithstanding these decisions there must be considerable doubt concerning the extent to which the erasure of data or programs stored as electrical impulses can be argued to be damage to tangible property as required by section 10 of the act. The unsatisfactoriness of this position led to the Law Commission (1989) rejecting the extension of section 10 to include data and programs in favour of a new offence, which was enacted in the Computer Misuse Act.

(v) Criminal Law Act 1977 retained the common law offence of conspiracy to defraud. Although the scope is wide, as was confirmed in Scott v Metropolitan Police Commissioner, it cannot be committed by a person acting alone.

As well as a knowledge of possible offences, which may be committed by a criminal using a computer, computer forensics also requires a knowledge of the law of evidence. Evidence in English law is categorised as either being direct or indirect (hearsay) and under common law only direct evidence is admissable.

Criminal evidence rules related to the admissability of documents stored on computer are contained in the Police and Criminal Evidence Act 1984 and the Criminal Justice Act 1988. The Criminal Justice Act 1988, s. 24 provides that documents arising from trade, business, professional, occupational or official activities which record information supplied by a person who has personal knowledge of the matters are admissable if the maker of the statement cannot reasonably be expected to, remember the matters contained in the record as would often be the case in computer environments. Further, as was held in R *v* Minors (1989) a computer produced statement must also meet the requirements of the Police and Criminal Evidence Act 1984, s.69 which states that:

(i) no reasonable grounds for believing that the statement was inaccurate due to the improper operation of the computer; and
(ii) the computer was operating properly, or if not that any irregularities would not affect the statement's accuracy.

The evidence must be certified. The certificate must specify the document, describe how it was produced including details of the equipment, state that s.69 requirements are met and be signed by a person responsible for the operation of the computer. The court is empowered to require oral evidence to support submissions but is unlikely to do so unless the accuracy of the matters certified is disputed.

These provisions give the defence considerable scope for shedding doubt on the computer derived evidence.

Another area of contention is authentication of the evidence (a print-out may be authentic in that it was produced by the computer even if it proves to be inaccurate or unreliable). There are no English cases which deal directly with the authentication of evidence derived from a computer. The closest case is R. *v* Maqsud Ali (1966), which centred on a tape recording in an obscure Punjabi dialect. A translation prepared for jurors (a parallel may be drawn to the transcription of magnetic into printed output) was acceptable provided the voice was properly identified and the accuracy of the recording was proved. However the judge gave the caveat that "Such evidence should always be regarded with some caution and assessed in the light of the circumstances of each case." The US position in the Federal Rules of Evidence is more relaxed. The requirement in rule 901(a) is "evidence sufficient to support a finding that the matter in question is what the proponent claims" and interpretations, as in US *v* Velda (1982), suggest that "a level of authentication greater than that regularly practiced by the company in its own business activities go beyond the rule . . . ." A more rigorous approach it is argued is tantamount to a presumption that computer records are *prima facie* inaccurate.

In the practical sphere, where a computer has been used in the commission of a crime, steps should be instigated to protect and preserve and evidence. In 1988 R *v* McMahon collapsed because of a failure by the police to secure the computer disks, which held key evidence, in a satisfactory manner. Further, the possibility of mailicious or self-destruct features must be considered and files on the system should be saved prior to investigating the system to guard against

this. Further, access to the computer should be carefully controlled not only at a physical level but also by suspending all current passwords and reissuing new passwords to trusted staff.

Finally, computer forensics should involve co-ordinating efforts to recover funds stolen. Such activity is not primarily a police function, although they will obviously provide assistance, and therefore a defrauded firm will usually consult accountancy and legal specialists. In solving a computer crime the police will often attempt to trace the funds and if the funds are in the UK the police can apply for court orders to assist tracing them. Once found if the monies are in a bank account abroad the authorities may have the right to freeze the account but this step is not available under UK law although a High Court Judge may following an application from the prosecutor issue a Restraint Order as a prelude to obtaining a Confiscation Order from a Crown Court on conviction. This should enable some of the funds to be recovered. If the funds are abroad victim companies will have to pursue recovery through local legal processes.

8. COURT ROOM PRESENTATION SKILLS

Cases involving computer fraud and abuse often combine a need to absorb large volumes of data presented as evidence and to comprehend conflicting evidence, which is couched in the technical jargon of the computing and accounting disciplines. This can prove confusing to jurors and witnesses and reduce the likelihood of justice being dispensed in a rational and methodical fashion. To avoid hiding the issue rather than clarifying it when presenting volumes of technical data, computer forensic skills must include an ability to present evidence in an understandable form. This will involve the computer forensics practitioner in making appropriate use of information technology facilities like:

(i) Visual aids displayed on screen;
(ii) The storage, retrieval and display of processed financial data; and
(iii) The storage retrieval and display of document images.

However the use of information technology creates a number of problems:

(i) Proper notice must be given of the intention to use the graphic output so that defense evidence may be similarly presented.
(ii) The limited space and time in court and obvious cost factors mean that realistically defense and prosecution must share one system of projection. This raises the problems of access, security, confidentiality and compatibility.
(iii) The actual control of the projection system is a matter, which is far from clearly covered at present in the courts. In the UK it is almost unheard of for the defence to use this type of facility, the reasons may be costs, lack of appropriate skills, or simply tradition.
(iv) Not all courtrooms are suitable for the display of computer graphics, though when new courts are built now, this factor is often considered in their design.

Further there is a need for certain safeguards and standards of practice for example, access to all case documents, diagrams and charts on disc by the defence (unless the material is properly privileged). Nevertheless the use of information technology for display purposes can help an computer forensic practitioner in:

(i) Producing schedules combining figures from more than one document can be done 'on-line' using a spreadsheet or database package, so as to aid jurors in their understanding of how various figures have been arrived at.

(ii) Displaying more than one document or schedule at a time so comparisons can be made highlighting the relevant figures. The reduction in the volume of paperwork also reduces the problem of storage and security of documents used in court.

The ITAC Working Party Final Report highlighted the possibilities given by technology as follows:

> There can be no doubt that technology has a role to play, not only in serious and in other fraud cases, but in the wider criminal jurisdiction .... The beneficial effects of the proper use of modern techniques in an area such as the criminal trial are we suggest, clearly seen. If the challenges we have identified can be met the benefits that will result are likely to contribute to a marked advance in the continuing efforts to secure quicker and more efficient trials in the future.

The ITAC Working Party Final Report On Technology in Serious Fraud Trials, 1989.

Computer forensic practitioners could play a leading role in this process.

9. COMPUTING SKILLS

A fundamental principle of forensic science is the Principle of Interchange, which was propounded by Edmund Locard in 1910. The principle asserts that when a person commits a crime something is always left at the scene of the crime that was not present when the person arrived. In computer forensics the computer is the scene of the crime and computing skills will be needed to collect evidence left by the person committing the crime. The evidence will enable the investigator to identify that a crime or abuse is being committed, discover how the crime or abuse is being committed, reconstruct evidence in situations where the programmer has tampered with files and extract evidence from computer files.

The investigator needs a combination of the EDP audit skills and the system specific knowledge of a computer manager. The route to identifying that a computer fraud or abuse is taking place and linking the crime with an individual will depend upon individual circumstances but the following abilities may be pertinent:

(i) Scrutiny and testing of the operations and teleprocessing logs. The former contains relevant information such as runs made, interruptions to processing (technical frauds often involve the use of recovery procedures, file

recreations and restarts from check-points as a means of covering tracks and removing audit trails), transfers of programs to and from production libraries and the use of utilities such as 'zap'. While analysis of the teleprocessing log may reveal strange behaviour by authorised personnel or attempts from outside to gain access;

(ii) Examination of computer programs and comparison of source and object versions of programs to identify unauthorised coding. Packages, which aid the former operation by printing flowcharts of the program logic flow, are available;

(iii) Use of concurrent auditing techniques, which can test logic of programs in operation and highlight exceptional items. Examples include integrated test facilities, snapshots of transacts, extended records and system control audit review files;

(iv) Covert observation techniques like logging all accesses to a given CPU or waiting for an access from a given source and examining in detail the nature of the activities undertaken;

(v) Knowledge of modes of privilege access controls and concurrency controls and an awareness of how these controls can be rendered ineffective or circumvented;

(vi) Methods of tracing system accesses with the assistance of telecommunication service providers and the police. Powers under the Interception of Communications Act 1985 permit this with the permission of the victim. This right, which existed only for indictable offences, was extended to unauthorised access offences by s.14 of the Computer Misuse Act 1990; and

(vii) Application of computer assisted audit techniques and other audit software utilities. Expertise in recovery techniques is needed to facilitate the reconstruction of evidence. The appropriate technique will dependent upon the nature of transaction logging and back-up procedures used by the organisation. At a minimum there will be an input log, which holds details of transactions processed for a set period. This record will often be supplemented by movement journals containing for a defined period information like: beforeimages of the master file prior to update; afterimages of the master file post update; or change parameters of changed records unique identifers and pointers. In many situations vital evidence may be recovered merely by restoring items flagged for deletion on the database.

The greatest problems in reconstruction arise when a considerable period of time elapses between the crime being committed and reconstruction activity commencing, as the retention period of all logs is limited. The admissability of such evidence in UK courts is somewhat unclear at the moment, but these computer forensic procedures will assist prosecutions.

10. CONCLUSION

This paper argues that the moves by the police and consultancy firms to successfully enforce the new legislation against the increased threat of computer crime and abuse requires the bringing together of investigative, legal, courtroom and computing skills in an extension of forensic science. The term suggested for this new discipline is computer forensics. It remains to be seen whether a recognised discipline, applicable to computer crimes and abuses, emerges in the next few years. The authors believe that unless this is the case there will be a series of failed major prosecutions before the subject is seen to present unique problems, which require special treatment.

REFERENCES

Albrecht, W. S., Howe, K. R. and Romney, M. B. (1984) *Deterring Fraud: The Internal Auditor's Perspective*, The Institute of Internal Auditors Research Foundation.

Audit Commission (1990) *Survey of Computer Fraud and Abuse*, HMSO, London.

Bowcott, O. and Hamilton, S. (1990) *Beating the System*, Bloomsbury, London.

Comer, M. J. (1985) *Corporate Fraud* (2nd ed.), McGraw-Hill.

Council of Europe Committee of Ministers (1989) *Recommendation No. R (89) 9 of the Committee f Ministers to Member States on Computer-related Crime*, Council of Europe.

Cornwall, H. (1988) Hacking away at computer law reform, *New Law Journal* **30** (September).

Hoffer, J. A. and Straub, D. W. Jr. (1989) The 9 to 5 underground: Are you policing computer crimes? *Sloan Management Review* (Summer).

Hollinger, R. C. and Lanza-Kaduce, L. (1988) The process of criminalisation: The case of computer crime laws, *Criminology* **26**(1).

Law Commission (1989) *Computer Misuse* (Law Com. No. 186 Cm 819), HMSO.

Law Commission (1990) *Jurisdiction over Offenses of Fraud and Dishonesty with a Foreign Element* (Law Com. 180 Cm 801), HMSO, London.

Nasuti, F. W. (1986) Investigating computer crime, *Journal of Accounting and EDP* (Fall), 13–19.

Stanley, P. M. (1986) Computer crime investigation and investigators, *Computers and Security* **5**, 309–313.

Tapper, C. (1990) *Computer Law*, Longmans, London.

Walden, I. (1989) *EDI and the Law*, Addison Wesley, New York.