



Home Office

The police recording of computer crime

Patterns of Crime

Crime Reduction

Policing and Organised Crime

Criminal Justice System

Drugs and Alcohol

Offenders

Corrections

Immigration and Asylum

Social Cohesion and Civil Renewal

Economic Analysis and Modelling

The Research, Development and Statistics Directorate exists to improve policy making, decision taking and practice in support of the Home Office purpose and aims, to provide the public and Parliament with information necessary for informed debate and to publish information for future use.

Home Office Development and Practice Reports are produced by the Research, Development and Statistics Directorate.

For further copies contact:
Communication Development Unit
Room 264,
Home Office,
50 Queen Anne's Gate, London
SW1H 9AT.

Tel: 020 7273 2084
Fax: 020 7222 0211
E-mail: publications.rds@homeoffice.gsi.gov.uk

Visit our website at <http://www.homeoffice.gov.uk/rds>

© Crown copyright 2004
ISSN 1477 3120
ISBN 1 84473 488 9

The police recording of computer crime

Kathryn Hyde-Bales, Sheridan Morris and Andrew Charlton

Introduction

A number of terms are used to encompass crimes that involve computers in various forms. This research has adopted the term 'computer crime', a phrase commonly used in UK law enforcement alongside the term 'hi-tech crime'. The role of computers in the commission of an offence varies and it is around this role that most high-level definitions revolve. The following three categories are suggested – a computer can be the target of criminal activity (e.g. a website as the victim of a denial-of-service attack, or a stolen laptop) or it can function as an intermediary for crime, either as a *medium* or *facilitator*. As an intermediary, computer systems are viewed as acting as a buffer between offenders and their victims, affecting how an offence is undertaken or executed (medium) – the criminal *modus operandi*. Similarly computers can enable communications between offenders in a global, near real-time and relatively secure manner (facilitator). Computer as an offending medium considers the offender-victim/conspirator contact, whereas computer as offending facilitator considers the offender-offender contact. The difference between these categories is often a matter of emphasis. It is possible for computers to play both roles in a single offence such as an Internet e-commerce based fraud (medium) which may also involve significant online communication between offenders (facilitator).

Recorded offences

As computers and the Internet have taken an ever-greater role in modern society, so too has the potential for their abuse, as both tools of crime and targets of crime. Whilst government and law enforcement have recognised this increasing problem, there is, with few exceptions, currently no formal recording of crimes that involve computers and the Internet. Such information is the first step in enabling the nature and scale of the problem to be quantified. In the immediate term, data allow law enforcement and government to allocate resources accordingly when faced with competing priorities and other offences for which they have established data sets. In the longer term, recorded information on the number of incidents enables the identification of emerging threats and offending trends.

The absence of offence categories¹ in this area is because the law has traditionally taken a technology neutral approach to offences (e.g. fraud is fraud however it is committed). Whilst this approach helps ensure that legislation remains effective and does not become redundant as technology changes, the absence of any reference to the *modus operandi* of the crime in regard to the role of computers and the Internet, prevents government and law enforcement from identifying such offences from recorded crime statistics.

This paper seeks to contribute to the Home Office and law enforcement efforts in tackling the lack of visibility of computer crime offending, a situation that is hampering efforts to assess and tackle the problem.

1. The Computer Misuse Act 1990 is the only legislation that explicitly and solely focuses on computer crime..

Home Office Development and Practice Reports draw out from research the messages for practice development, implementation and operation. They are intended as guidance for practitioners in specific fields. The recommendations explain how and why changes could be made, based on the findings from research, which would lead to better practice.

Reporting crime

As well as visiting a police station in person to report an incident, victims of computer crime can contact the police through a number of channels. The force control room will generally take urgent (e.g. 999) or out-of-hours phone calls. Non-urgent calls during normal office hours will normally be routed to a force-wide, or more local (Basic Command Unit) crime desk (also known as crime management unit or similar). If a caller asks the police switchboard for a specialist unit they may sometimes be put in direct contact with units such as the force computer or economic crime (fraud) unit, though some forces have explicit policies not to do this. However, whilst these specialist units are found in all forces, most reports, including computer crime, are normally passed to local officers first.

A very small number of forces have websites to which information can be passed (see Online policing below). Members of the public can also report any paedophile or race hate content they find whilst online to the Internet Watch Foundation² (IWF). The Crimestoppers website³ also allows the reporting of any type of crime online, not just computer crime.

Recording crime

There are generally two recording stages when a crime or occurrence is reported to the police. First, an *incident record* is created that records basic details of the victim or caller, and the incident (e.g. offence type, location). This record is entered onto the force command and control system, the primary system used by force control rooms when taking calls from the public. The incident is then usually assigned to a uniform police unit on a geographic basis, normally local to the victim or caller, for initial investigation. Occasionally an incident will be passed directly to a specialist unit for investigation but this is not common. Incident records largely take the form of free text and are not assigned a crime recording code (see below) at this stage.

Once an initial incident investigation has confirmed that, on the balance of probability, a crime has been committed, a crime record is created on the force crime recording system – this is the second stage. This entry will use a local force code⁴ to record the offence type, e.g. obtaining property by cheque or credit card fraud would be the offence for an online purchase using a stolen credit card. A crime record will also record key information such as victim and crime details, as well as offender details if known. The crime record will normally also contain a variety of tick boxes known as codes, flags or markers, to record a variety of offender *modus operandi* details. A common example relates to burglary where markers may be used to record the point of entry, the means of entry and the means of exit. Other ad hoc recording markers exist to record an event as a racist or homophobic incident.

It should be noted that stage one, incident recording, may be omitted by some forces, e.g. those with a central crime recording unit attached to their central call centre who can create an immediate crime record.

Recording intelligence

A third repository of police crime information is the force intelligence system. This system will generally contain background intelligence on both known and suspected offenders, criminal events and certain police operations. As with the crime recording system, the intelligence system will make extensive use of coded markers. The examination and recording of a criminal's *modus operandi* is an established means of analysing and identifying (or short listing) offenders in criminal intelligence circles. Such information is used to identify potential suspects who may use a distinguishing *modus operandi*, and also to keep abreast of new means of offending generally. Such information can also be used proactively to alert potential victims to new criminal techniques.

2. www.iwf.org.uk

3. www.crimestoppers-uk.org

4. Although forces may use their own codes (e.g. 127) for an offence, each code records a national Home Office offence category, which has its own Home Office classification code (e.g. 53A is the code for obtaining property by cheque or credit card fraud).

Computer crime *modus operandi* marker

There are then three primary sources of data (incidents, crimes, intelligence) that record events brought to the attention of the police. In the absence of relevant crime recording codes, the primary potential means of identifying computer events will be through the use of suitable *modus operandi* markers or codes. Thus incidents as varied as credit card fraud or the distribution of paedophile images could both be identified as computer crime by simply filtering all incidents where the computer crime marker has been ticked on the information system.

An alternative but less effective means of searching for such incidents is by the use of a free text search on plain text fields in the recording systems (e.g. searching for any use of a relevant word like 'Internet' or 'computer'). It is the use of these codes and text search capability that the survey primarily sought to identify.

Aims of the research

The research aimed to find out if it was possible to identify computer crime from force information systems through the use of suitable markers and/or the use of free text searches. To do this the survey examined how forces are recording and allocating computer crime incidents.

Methods

The recording practices for instances of computer crime were examined for all 43 geographic forces in England and Wales. The survey was broken down into three stages. The initial stage acted as a scoping exercise in which five forces were visited. The second and third stages involved 20 telephone interviews and 18 postal surveys that were conducted in parallel during June and July 2003. During each stage, the following six areas were examined as they represented the primary areas in initial incident handling, crime and intelligence recording, and specialist computer crime policing:

- force control room;
- crime desk;
- force intelligence unit;
- child protection unit;
- fraud/economic crime unit; and
- hi-tech/computer crime unit.

Representatives from each of the six areas within each force were interviewed or completed a postal questionnaire. Department respondents were nominated by the force and varied by rank for similar areas (e.g. force control room respondents varied from civilian call operators to duty Inspectors). Thus there was sometimes a variation in the knowledge possessed by respondents, though any outstanding questions were resolved by subsequent correspondence.

Additionally, a web survey of force websites was conducted to examine their capability to accept online incident reports.

Findings

Two hundred and twenty-four questionnaires were completed out of a possible 258. Twenty-two forces completed all six questionnaires, with a minimum of three questionnaires received from every force.

Incident recording (force control rooms)

- Only one force (3%) had a computer crime marker they could assign to command and control incident records. The force did not, however, have any documented guidelines on its use.
- Only one force (3%) reported they could execute a free text search using key terms such as 'Internet' to identify computer incidents on their command and control records.

Recording and identifying computer crimes (crime desks and others)

It was found that in addition to force crime desks, a variety of other units and individuals could create entries to the force crime recording system.

- Eight forces (13%) said their force control room could create crime records.
- Sixteen (25%) forces said their local police station personnel could create crime records.
- Eight (13%) forces said a number of special units could create crime records.

Such variety of record creation provides both opportunities and weaknesses for an effective computer crime policy. As the public may notify forces of incidents in a number of ways then it is important that all those dealing with such incidents are able to detail and code incidents accordingly. The weakness of a diversified data entry system (in contrast to a single central data input team) is that the maintenance of data quality becomes more difficult in the absence of effective training and documented guidelines, particularly in regard to less common crimes such as computer crime.

Having established who created records, the survey then examined to what extent crimes with a computer crime *modus operandi* could be recorded.

- Eight crime desk respondents (23%) reported their force had a computer crime marker they could assign to crime records. Five with computer crime markers reported having documented guidance on their use.
- Twenty-four force crime desk respondents (65%) reported their force could execute a free text search on key terms such as 'Internet' to attempt to identify computer incidents.

The ability of forces to mark crime records as featuring a computer crime is essential for subsequent identification and analysis of crime record data (e.g. to identify number, trends and forms of computer crime).

Recording and identifying computer crime intelligence (force intelligence unit)

Just as with crime records, the ability of forces to mark intelligence records as featuring a computer crime element is essential for subsequent identification and analysis of crime record data. Again, intelligence unit information may be used to examine the level and form of offending a force is faced with, as well as identifying offenders known, or suspected of, being involved in some form of computer crime.

- Eleven forces (31%) reported that they had a computer crime marker they could use to identify computer crime related intelligence logs (two didn't know, 23 said no). Only Six of these forces reported having documented guidance on its use.
- Twenty-three forces (64%) were able to execute a free text search on key terms such as 'Internet' to identify individuals involved or associated with computer incidents; the rest could not.

Recording computer crime

- ✓ Forces should implement a computer crime marker on both their crime recording and force intelligence systems (and consider a similar implementation to incident systems also) to enable the identification and subsequent analysis of computer crime incidents, crimes and offenders.
- ✓ Such a marker should be accompanied by documented guidance on its application.
- ✓ Individuals, who undertake analysis of incident, crime and intelligence data would benefit from receiving specific training on the key aspects of computer crime.

Handling computer crime incidents

Force control room

As one of the initial points of contact on receiving calls, force control rooms were asked for which computer crimes, if any, they had documented guidance on allocating. Of the thirty eight respondents:

- Four forces (11%) reported having guidance on Internet-related fraud incidents;
- Five forces (13%) reported having guidance on online paedophilia incidents (e.g. images); and
- Four forces (11%) reported having guidance on hacking incidents.

Crime desks

Crime desks are also often an initial point of contact with the public, allocating incidents, as well as being the major unit responsible for entering incidents into the crime recording system. Respondents were asked what training they had received in regard to computer crime.

- Only one force respondent (3%) reported receiving training in computer crime.

Call handling computer crime incidents

- ✓ Documented guidance on computer crime categories, accompanied by basic training on the key aspects of computer crime, should be given to all individuals involved in call handling so as to ensure the timely and accurate allocation of computer crime incidents.

Online policing

All 43 police forces in England and Wales have public websites, which were examined as part of the research. As well as being a means of providing information to the public on matters as diverse as police authority business plans and police recruitment, they can also serve as a means of online crime reporting and capturing valuable criminal intelligence from the public.

Non-emergency minor crime notification

The online Non-Emergency Minor Crime Notification website⁵ is administered nationally by the Police Information Technology Organisation (PITO). Although this site can only be used to notify forces of four crime categories (theft, criminal damage, theft from a motor vehicle and damage to a motor vehicle), and hence not relevant to reporting computer crime, it is perhaps the most sophisticated online system currently available. It collects crime and victim information in a detailed and structured manner, and then forwards it to the relevant force. Thirty-two (75%) forces' websites provide this service by placing a link on their website. It should be noted that whilst some forces featured the link prominently on their homepage, it had to be searched out on others.

Force Computer Crime Notification

Only three force websites had mechanisms for reporting computer crime. One force⁶ had an online free text form that was sent directly to its computer crime unit for any kind of online crime. More specifically, one force used an online free text form for reporting paedophile-related issues⁷, whilst another gave an email address for providing details of email fraud scams to its fraud unit⁸. It may be that other forces had similar services but these could not be found. The provision of such online notification must be accompanied by a reliable back office process to ensure it is allocated and responded to in a timely and accurate manner.

Eleven forces provided links to the Internet Watch Foundation (IWF) website where members of the public can report paedophile websites, or other content, they believe to be illegal. The IWF also accepts notifications regarding racist material, though most forces did not mention this.

Website feedback

Whilst only a small number of forces have any kind of formal means of reporting non-urgent incidents as detailed above, 18 websites contained details for contacting the webmaster. Whilst this address is designed to receive feedback regarding any problems with the website, interviews with forces indicated the public were using such email addresses to inform forces of criminal incidents or other intelligence. Thus websites were inadvertently becoming another means by which forces were being alerted to criminal incidents. Of the 10 force webmasters who replied to the questionnaire:

- seven had received emails from individuals who felt they had been a victim of an Internet-related crime;

5. <http://www.online.police.uk/english/default.asp>

6. Avon and Somerset Constabulary.

7. The West Midlands Paedophile Unit takes online notifications regarding paedophile images, online grooming and sex tourism.

8. Thames Valley Police.

- eight had received emails providing information regarding an Internet offender or other criminal activity; and
- five had formal guidelines on what to do upon receipt of any emails regarding an Internet offender or other criminal activity.

The lack of formal guidance to individuals who are receiving, albeit inadvertently, criminal intelligence and incident reports, is of particular concern in that such individuals were based in non-enforcement departments e.g. IT, corporate affairs, press office, public relations.

Force websites management

- ✓ Forces should give consideration to providing the public with a clear online means of reporting crime and information via the established non-emergency minor crime notification and IWF schemes.
- ✓ Internal procedures on the handling of computer crime emails should exist for force webmasters so as to ensure the timely and accurate handling and allocation of computer crime incident reporting and intelligence.

Hi-tech crime awareness

As the Internet and computing increasingly permeate everyday life, so will its criminal abuse enter the day to day policing challenges faced by all officers, not just specialist officers. Whilst new probationary and CID officers may receive an element of computer crime training, there is still an essential role for raising the awareness of existing officers and staff. For this reason, the survey also examined to what extent specialist computer crime units were involved in promoting awareness and knowledge throughout their force. It was found that a number of specialist units provided computer crime training for others within their force.

Computer crime units gave training to the following areas:

- Probationers – 19 (50%)
- CID – 22 (56%)
- Senior Investigating Officers – 15 (39%).

Economic crime units gave training to the following areas:

- Probationers – seven (18%)
- CID – six (16%)
- Senior Investigating Officers – six (16%).

Whilst it is essential that all police personnel receive foundation training in computer crime, and it is encouraging to see that specialist units are seeking to contribute to this need, such training clearly represents a distraction for operational units. The National Specialist Law Enforcement Centre (NSLEC) has produced a computer crime module for the probationer training programme and provides numerous advanced modules for specialist units such as, computer crime, fraud and child protection.

Other means of raising awareness of what, and how, crimes may be reported clearly exist outside training. For example, the Internet Watch Foundation has produced a leaflet for distribution amongst the public and police front-counter staff, explaining what material can be forwarded to them and through what channels. Such simple initiatives should contribute to raising awareness in at least one important area of computer crime.

National hi-tech crime unit operational protocol

The current absence of, and reasons for, reliable England and Wales computer crime statistics has been discussed. To attempt to overcome this problem, an operational protocol signed between the NHTCU and its strategic stakeholders⁹ in 2002 included an agreement for national computer crime reporting and collation. This agreement was based on the stated national need to 'gather reliable statistical data on computer crime to assist in measuring the threat, benchmarking performance, prioritising activity and informing future resourcing requirements.' It was

9. The Police Service in England and Wales (ACPO), the National Criminal Intelligence Service (NCIS), the National Crime Squad (NCS) and HM Customs & Excise (HMCE).

agreed that 'all parties should capture data on their respective intelligence and crime reporting systems in a way that enables the computer element in crime to be recorded, retrievable and analysed.' This research has shown that forces currently do not have this capability.

The agreement also required that 'parties without this capability undertake to review arrangements and include this requirement in future plans. The parties acknowledge this as a priority action.' This survey sought to review progress towards this protocol and asked force crime desks, force intelligence units and computer crime units if they were aware of the protocol requirements in regard to national recording. The following were aware of the protocol:

- Four (13%) crime desk respondents;
- Fourteen (43%) force intelligence unit respondents;
- Twenty-nine (86%) computer crime unit respondents; and
- Twenty-two (67%) economic crime unit respondents.

Computer crime and economic crime units were asked if they maintained an activity log or record of their activity.¹⁰

- Thirty-seven (95%) computer crime units maintained their own case logs.
- Sixteen (42%) economic crime units maintained their own case logs.

Anecdotal evidence showed a wide variety in the format, detail and accessibility of such records. Common formats were excel tables but a variety of databases were found, as well as basic paper ledger books. It is suggested that such locally based records should not be considered as reliable and accurate sources of data of force-wide computer crime activity.

The protocol requires force computer crime units to submit crime data electronically via the NHTCU Extranet on a monthly basis.

- All but one (98%) computer crime unit had the required access to the NHTCU Extranet.
- Twelve (32%) economic crime units had access to the NHTCU Extranet.
- Four (12%) force intelligence units had access to the NHTCU Extranet.

As of July 2004 no data had been submitted to the NHTCU from local computer crime units as per this protocol. It is suggested that the identification and submission of computer crime statistics to the NHTCU not be a task of computer crime unit officers, but rather the force statistics officers who are currently responsible for submitting crime data to the Home Office. The small number of officers trained in tackling computer crime should not be diverted from their primary task to undertake a function best undertaken by others who are equally trained in the specialism of data collation, evaluation and analysis (e.g. crime recording staff and intelligence analysts).

Moving forward

National initiatives to record the computer crime facing the UK must be built on local developments, namely the development of force recording systems as discussed. As the tackling of computer crime incidents should be seen as a function of mainstream policing, its recording should use the standard information management systems as discussed, rather than improvised, stand-alone systems managed solely by computer crime units. In the absence of a raft of new legislation identifying specific computer crime offences (in contrast to the current technology neutral approach) which would then require Home Office notification, it is suggested that the first step is for forces to implement a computer crime *modus operandi* marker on recorded crimes as previously outlined. This research has shown that even such a basic measure is not yet in place. At the time of writing, discussions between local force crime registrars, the NHTCU and the Home Office were seeking to encourage this development. Although national data analysis is built upon local data capture, it may be that a national requirement is necessary to ensure forces undertake such measures, as per the current provision of data collated via the Home Office annual data requirement process for other crime categories. This is particularly relevant due to the sensitivity of any recorded crime performance measure in reviewing and comparing force statistics.

10. The survey also questioned child protection units about online paedophile incidents. It was found that there was no clear allocation of incidents to such units, with local CID, rather child protection units, often dealing with such incidents. Therefore the responses from child protection respondents are not discussed as they are not considered as representative of the police service response to such incidents.

Such local recording of computer crime incidents could directly contribute to a national understanding of the problem through the National Management Information System (NMIS), an ongoing PITO initiative. Under NMIS, information from disparate force systems is combined in a data warehouse from where it can be analysed and presented in a consistent format. By enabling the sharing of data and analysis at a national level, the police could provide an enhanced proactive response to national crime trends. On an international basis, the Interpol European Working Party on IT Crime has been working on a common computer crime classification system, enabling the comparison of incidents and crimes between countries through the use of common categories.

Such technology developments must be accompanied by adequate process documentation and staff training for personnel across a wide variety of functions, such as call handlers, crime desk inputers, intelligence analysts and operational patrol officers. The role of force crime registrars in overseeing the standards of crime recording is acknowledged, their role drawing upon extensive training, experience and detailed guidelines to ensure recording accuracy. National bodies such as National Specialist Law Enforcement Centre have developed a number of specialist courses, though forces could adequately train information system staff on the elements of computer crime relevant for their role.

Alongside force recording measures, consideration should be given to expanding the existing non-emergency minor crime notification system to include a number of computer crime categories. Such offences are likely to be experienced or witnessed by the online public, so it seems natural that they may be inclined to use online reporting tools where available. Such a centralised system would also serve to capture at the outset, computer crime incident reports, although their verification would follow afterwards at a local level.