



THE EUROPEAN
INFORMATION
SOCIETY GROUP

EURIM



EURIM – IPPR E-Crime Study
Partnership Policing for the Information Society
Working Paper
Roles and Procedures for Investigation

The Issue

E-crime can be described simply as crimes that require ICT expertise during investigation and can range from:

- Crimes made more efficient by using computers and the Internet to gain access to larger numbers of potential victims at lower cost/risk to the perpetrator. Examples include auction fraud, identity cloning, mis-selling and paedophilia.
- Conventional criminal activities managed through use of electronic services. Examples include the use of email, mobiles, search engines, funds transfer et al in support of blackmail, fraud, extortion, drug or people trafficking.
- Attacks on computer systems themselves. Examples include viruses and denial of service. Many of these look to victims like familiar crimes such as vandalism (e.g. defacing web sites) or criminal damage (e.g. causing a computer to crash).

Crimes involving ICT systems are now commonplace. Consequently, in a wide variety of crimes there are new opportunities for intelligence gathering and investigation which exploit information in digital form, even where a computer is neither the target of attack nor the primary tool to commit the crime. As a result:

- New skills are required at all levels within the police and supporting services to enable investigators and forensics experts to trace and analyse criminal activities that involve computers and networks and to gather intelligence from them.
- New and different techniques are needed to ensure the provenance of evidence in digital form.
- The sheer volume and complexity of such evidence itself also places greater burdens on the resources required to undertake such investigations – billions of characters of data are being seized in a single case

Crimes using computers give criminals the potential to affect huge numbers of potential victims at low cost and risk, with a consequent potentially large increase in the numbers of reported incidents. As an example, recent spoof high street banks' emails and web sites caused many people to provide details of their bank accounts over a very short time – something that would have been very difficult without the Internet. The ability of law enforcement to cope with this level of activity is further impacted by the significant extra cost of investigations that involve digital evidence. Investigating a fraud perpetrated electronically requires significantly different skills, and potentially greater resources, than investigating a bank robbery, for example, leading to greater pressure on balancing priorities between cleanup rates and cost of investigations. It will take a significant time to train sufficient people with the right capabilities to handle every reported incident involving computer systems – even if there is the political will and sufficient funding. Current resourcing levels are sufficient to enable only major incidents to be investigated, resulting in a backlog of reported incidents that are not being addressed.

Unlike physical crimes, it is often difficult for the victim of a computer-enabled crime to determine that a potential criminal act has occurred without significant preliminary investigation. It is obvious when the office has been broken into and vital files stolen, it is less obvious that someone has taken a copy of the bank account details stored in your computer. Even where a suspicious event is detected in a computer system, some basic analysis is necessary to eliminate other possible causes, such as accidental user actions, product faults or system administration errors. If this is not done to appropriate standards the provenance of any electronic evidence may have been compromised before the suspicious event has even been reported. Many potential victims, especially SMEs and other small organisations, do not have the appropriate skills to carry out even this basic level of analysis, leading to the reporting of incidents that turn out not to be criminal activity or that cannot be pursued because evidence has been tainted.

There is always debate on the relative priorities for law enforcement given that there is not unlimited resource. Current priorities are focused on visible social issues, such as burglary, car theft and public disorder, on the one hand and major international criminal activity, such as drugs, people trafficking and paedophilia, on the other. White collar crime is already suffering from lack of resource within law enforcement with only major crimes being investigated. For example, cases of fraud are only likely to be investigated where the sums involved are large. The way law enforcement is organised means that most crime is reported to the local police forces who are not resourced to handle it, nor are they motivated by the National Policing Plan or Performance Indicators to invest resource in doing so. As a result some industry sectors are already taking greater responsibility for the investigation and prosecution of some types of crime. Examples are the actions by the software and entertainment industries to combat piracy and illegal copying.

There are significant investigative and forensics resources already employed in industry, both within large corporations (some of whom have more network investigators and computer forensic staff than law enforcement) and within specialist security and risk management firms. These do work to appropriate standards, and have developed close working relationships with the police. This is especially true of Financial Services organisations, Telcos and ISPs, but such arrangements are largely ad-hoc. They also affect only the larger organisations, and not smaller ones such as SMEs.

There are no current indications that law enforcement priorities or resource levels related to the investigation of e-crime will change significantly in the immediate future. However, the Home Office Consultation Paper, *Policing: Building Safer Communities Together*, published in November 2003, does include potentially significant proposals for changes to the way society is policed. In particular it discusses ideas included in this, and other, papers in the EURIM-IPPR E-Crime Study. The private sector will continue to invest significant resource in the investigation of computer-enabled criminal activities as it affects their businesses, often working closely with law enforcement. If the UK is to maintain its leading position in the emerging digital world we need to find ways for industry to work with and support law enforcement by developing better co-operative ways of working to combat e-crime.

The Approach

Large organisations in some sectors (such as financial services) already have significant investigative capability, and working relationships with law enforcement. However, the increasing business and private use of computer systems is exposing many more users as potential victims of e-crime, requiring support organisations to investigate how systems they support have been exploited for criminal purposes. There are long term changes that can be made to improve the ability of all involved in tackling e-crime, but there are also immediate measures that could be taken to help those faced with potential e-crime related incidents in two areas:

- The guidelines, standards and procedures under which suspicious incidents are handled.
- The introduction of professional training and standards for those involved in investigations.

Guidelines, Standards and Procedures

Guidelines and standards are required at two levels. For the great majority of organisations a simple set of procedures is needed that people such as systems administration staff, support staff and network managers can follow if they suspect a criminal incident. This should be aimed at minimising the risk of evidence being compromised, enabling sufficient information to be collected to support a sensible suspected crime report and advising on how and where to make such a report while minimising impact on the business while the computer system is being investigated. Basic guidance

on key legal aspects would also need to be covered – such as the legal position when paedophile images are found or matters relating to the protection of personal data. The guidelines would not enable detailed investigations or computer forensics to be undertaken.

There are already sources of such information¹. Assembly in a form suitable for distribution to different constituencies could be included as an extension to the work proposed on common sources of information in the EURIM-IPPR paper on [Addressing the Needs of Small Firms](#). Distribution could be through the channels identified in the same paper.

Recommendation 1

Develop a core set of simple guidelines for those involved in managing and supporting computer systems, especially in smaller organisations such as SMEs, advising on what steps to take where they suspect criminal activity on their systems before they report it to the relevant authorities. This should build on recommendations in [Addressing the Needs of Small Firms](#).

The EURIM-IPPR paper on [Reporting Methods and Structures](#) discusses how people should be able to report suspicious incidents. It supports the work being done by the ICF “One Stop Shop”, PITO, the NISCC and the NHTCU in creating portals for the reporting and routing of potential criminal incidents. However, not all victims will be able or want to report incidents on-line in which case they will usually report them to their local police desk – typically in person or by telephone. Those manning these desks will need to be trained to help callers, working from simple guidelines, directing them to the most appropriate place to handle the incident. This may well be not a law enforcement agency² but, for example, a PC support service. This requirement could be met by providing those manning front desks, after appropriate training, with guides and decision trees based on those being developed for small firms.

There are organisations that already carry out significant investigation of potential criminal incidents before involving the police, or retain an outside company to do so on their behalf. Their staff often continue to assist the police once they have become involved. The private sector is prepared to invest in the provision of appropriate skills where they are dedicated to addressing crimes in specific areas. The Dedicated Cheque and Plastic Card Crime Unit (DCPC), a joint operation between law enforcement and the financial services industry, is largely staffed and funded by industry, but operates under a law enforcement remit. This avoids the major barrier to private investigation and prosecution of criminal activity – the frequent need at some stage in an investigation to use techniques that are only permitted to law enforcement and similar agencies. Examples are access to personal data and the ability to seize relevant information. Given the resource constraints within law enforcement, there would be advantage in encouraging similar joint operations in other areas subject to specific types of criminality such as insurance, counterfeiting and telecoms, with private industry providing the bulk of the expert resource/funding under a law enforcement remit.

Recommendation 2

That the creation of joint private industry/law enforcement crime units along the lines of the DCPCU be encouraged. The Home Office should convene a workshop involving interested parties to decide how to establish guidelines for the creation, governance and operation of such joint crime units.

Whether working within such joint crime units or independently, private sector investigators and forensics teams will, inevitably, reach a point where law enforcement agencies need to become involved. There are actions that only law enforcement are authorised to undertake. Examples are access to personal data or to information held by third parties. Informal processes already exist in particular sectors, notably financial services, to achieve this. However, as the private sector investigations increase in number and scope there is a need to formalise the way such requests are

¹ For example, the documentation on www.cert.org/nav/allpubs.html, although it would need to be adapted to include UK and European, rather than US, law and regulations.

² Where “law enforcement agency” here includes a broad range of agencies with legal powers of investigation including Trading Standards, Health & Safety, Customs & Excise, Inland Revenue, and the Benefits Agency.

handled.

Recommendation 3

ACPO(?) develop guidelines with industry for handling requests from private investigation teams for supporting services for which only law enforcement are authorised. As an initial step the NHTCU could investigate what procedures and guidelines are already available.

To assist in joint working, whether within a formal structure such as the crime units mentioned, or just as part of normal interactions between law enforcement and private sector investigation teams, all those involved in investigative and forensics activities should work to a common set of standards and guidelines – even possibly using common preferred sets of tools. ACPO has already accepted in principle that Guidelines it produces could be made more widely available to encourage their use across the private sector. The revised ACPO Good Practice Guide for Computer based Electronic Evidence³ has just been published and is a first step in this direction. There are other guidelines and standards that are being developed, including one for network investigators. While care needs to be taken that sensitive material relating to operational procedures is removed, there would be significant benefit in their wide publication. It would enable those in the private sector to work to the same standards as those in law enforcement, facilitating exchange of evidence and information. It would also make it easier for law enforcement to take over investigations confident in the knowledge that the work done to date had good provenance. It would make it easier for those in the private sector to decide when to call in the law enforcement agencies in a way that ensures the case can be prosecuted successfully. If maximum benefit is to be got from sharing such documents, it will be necessary to train those in the private sector in their proper use. This is discussed further under *Certified Practitioners* below.

There are many guidelines, practices and tools used across the private sector from which law enforcement might benefit. Processes should be set up whereby those in the private and public sectors with common interests can meet on a regular basis to exchange views and experiences, develop and refine common guidelines and standards, and exchange information on tools and techniques. Although this happens at the moment to some extent, it is informal and does not fully involve all those with appropriate experience. A good example is the Digital Evidence Group, a Home Office chaired working group, which aims to contribute to the development and delivery of high quality forensic recovery and examination of digital evidence throughout the various UK Law Enforcement, Government Department and associated agencies. Digital storage means that vast quantities of data are being seized in a small number of cases. DEG is looking at the impact of this on disclosure in the context of the Criminal Justice Bill and wider work on disclosure.

As the capacity in industry to undertake such work increases, and other industry sectors become involved, there would be advantage in formalising this information sharing process to encourage the sharing of experience and the wide take-up of best practice methods and tools. The EURIM-IPPR paper on [Reporting Methods and Structures](#) includes recommendations for the sharing of incidents, information and intelligence between communities based on the WARP (Warning, Advice, and Reporting Point) scheme being developed by NISCC. This could be adapted to create a similar set of community-based schemes for sharing information on investigative and forensics best practice and associated topics.

Recommendation 4

That the NHTCU develop a scheme similar to the WARP scheme being developed by NISCC for the exchange of investigative and forensics experience, best practice and tools within communities

The NHTCU is developing an Industry Outreach policy. This should include advice and guidance to those in industry on when to involve law enforcement in investigation of suspicious incidents. It could also provide references to the key guidelines, standards and best practice documents that industry should use.

³ Available on www.nhtcu.org

Quick Win

Publicise, and actively encourage the use by those in industry involved in investigations, forensics, etc Guidelines, Standards and Codes of Practice used by law enforcement relevant to handling investigations, linked to appropriate training.

The NHTCU Industry Outreach Policy may be a vehicle for this.

Certified Practitioners

There are currently no widely recognised computer-related qualifications for a wide range of people across the criminal justice system, including particularly investigators, computer forensic experts and lawyers. If there is to be trust and sharing between people with appropriate skills and competence in their application across the public and private sectors, and possibly internationally, there would be real benefit in having accredited qualifications that are universally acknowledged. There are moves in this direction with organisations such as, for example, the Institute for Computer Arbitration and Forensics (ICAF) and the Council for the Registration of Forensic Practitioners (CRIP), but no widely acknowledged criteria or qualifications across the full range of skills. There are people providing training in specific skills in both the public and private sectors – notably within national police training (NSLEC) and in certain higher education establishments (such as Cranfield University-RMCS, University of Glamorgan and Royal Holloway). However, the quality of this training can be variable, and content can be specific to the target audience. There is also a need to certify that an individual has not just the requisite knowledge, but also the ability and experience to apply that knowledge effectively. The EURIM-IPPR paper on [Growing the Necessary Skills](#) includes recommendations relating to these skills training issues. It is not yet clear what role the soon to be announced Criminal Justice Sector Skills Council (JSSC) might play in establishing appropriate certification criteria.

Law enforcement does not have, and is unlikely to have in the foreseeable future, the capacity to handle all potential incidents if they were reported. Recent high profile investigations of computer-related criminal activity (e.g. paedophilia) show how the resource available can be swamped by the capacity of e-crime to generate huge numbers of victims as well as volumes of data to be sifted. Building on the previous recommendations that information on guidelines, etc be shared between the private and public sectors, possibly as part of joint crime units, it would further reduce the load on law enforcement if investigations in the private sector could be carried out by people accredited to be working to standards and procedures commonly recognised across the public and private sectors. This approach can be used to maximise the use of scarce skills in industry in support of law enforcement activities from investigators to technical experts – indeed in the USA people with particular skills already undergo appropriate training by the FBI, for example, and are called in on specific cases to provide specialist expertise to investigation teams.

In the early stages of this study the idea of Specialist Constables was floated. This generated considerable positive discussion. There was a general view expressed that such an approach could make investigation and prosecution of criminal activities easier and cheaper, and encourage joint working between industry and law enforcement in combating e-crime. However, there were concerns over whether it was the right model (images of “special constables”). It appeared there might be greater benefit from schemes linking certified qualifications to a range of skills or competencies, including knowledge of relevant legal and regulatory matters, relevant law enforcement practices and appropriate working practices. There was also a view that different situations might require different types of co-operation and governance routines. One size would not fit all. The Consultation Paper on Policing includes in Paragraph 4.21 consideration of this idea.

While the sharing of information can be done quite easily, the certification of people as having specific skills and competencies that enable them to work closely with law enforcement is a far more complex issue. It will require significant discussion across law enforcement, government and industry to agree the scope of the competencies required. It may require changes to laws or regulations. It will almost certainly require formal statements covering the responsibilities and liabilities of the various parties when working together. Further consideration of the legislation and regulation aspects can be found in the EURIM-IPPR paper on [Legal Issues](#)

Recommendation 5

The Home Office to investigate with representatives of law enforcement, industry, and other interested parties the possibility of investigators and others in industry with appropriate skills

and experience being accredited to work to the same legal and operational standards and guidelines as law enforcement when involved in e-crime investigations (possibly building on work done in the past by the Fraud Squad).

© Copyright EURIM 2003. All Rights Reserved. For written permission to reproduce any part of this publication please contact the Administrative Secretary, EURIM, (email: admin@eurim.org; fax 01984 618383). This will normally be given provided EURIM is fully credited. Whilst EURIM has tried to ensure the accuracy of this publication, it cannot accept responsibility for any errors, omissions, mis-statements or mistakes.