



THE EUROPEAN
INFORMATION
SOCIETY GROUP

EURIM



EURIM – IPPR E-Crime Study
Partnership Policing for the Information Society
Third Discussion Paper

Supplying the Skills for Justice
Addressing the needs of law enforcement and industry
for investigatory and enforcement skills

1) Introduction - Why Action is Needed

10% of the population of the world is now on-line, including half the population of the UK. So too is a similar proportion of criminals. The criminals are achieving significant economies of scale in automating old crimes - one example is the £150 million lifted from the DfES Individual Learning Accounts. They are also inventing new ways of committing those crimes - for example replacing arson by denial of service attacks to support extortion rackets.

We have around 140,000 police officers in the UK. Barely 1,000 of them have been trained to handle digital evidence at the basic level and fewer than 250 are currently with Computer Crime Units or have higher level forensic skills. Add in the civilian staff of the Forensic Science Service and its contractors and the pool of full-time expertise is still under 400. No wonder we have forensics backlogs of 6 to 12 months and reluctance on the part of most local forces to launch any new investigation. Until very recently, Operation Ore¹ took up most of the resource available save when displaced by the murder or terrorist investigation of the day, such as Operation Crevice², which involved a massive diversion of NCS resources. Computer assisted extortion, fraud and impersonation, however great the damage, are on the back burner. Any attempt to change the situation requires change to both the skill levels available and the priorities for deployment.

Meanwhile there are estimated to be about 8,000 security "experts" in the private sector. These range from former members of the armed forces, police and security services, now with budgets and technologies to which they rarely had access before they left the public sector, to former hackers with uncertain skills and/or motivation. **Law enforcement is facing a crisis: unless we act rapidly and effectively to address the mismatch between task and skilled resources, we face a very real risk of seeing the democratically accountable policing of computer-assisted crime replaced by a combination of vigilante action and the covert privatisation of legitimate investigation.**

One of the first areas where activity is needed is the "sizing" of the skills requirement. The current focus of UK skills and training in Computer Security and Forensics is on low cost courses to address low level skills (NVQ2 and below) at one end of the scale and on high level (graduate and post graduate) skills at the other. Meanwhile the crises are in the middle, technician level skills (NVQ level 3). Moreover, sub-NVQ, mass-market training is also missing, the throughput of the high level

¹ Operation Ore investigated the supposed holders of 7,000 UK credit card numbers allegedly used to pay for access to an American paedophile website.

² Operation Crevice involved the diversion of 700 police officers in March 2004 to assist in the arrest of several people suspected of planning a large explosion in an urban centre.

courses is seriously inadequate and responsibility for action is fragmented across sector skills councils and other bodies, often with overlapping interests and usually with un-coordinated plans. The problem is recognised in the *Police Sector Skills Foresight 2004* report: "With the notable exception of fingerprint experts, the implications on resources are a matter of development and deployment of appropriate levels of expertise, rather than a demand for increased resources."³

Government policy is for an employer-driven skills training and qualifications system. However, with regard to the skills needed to combat computer-assisted crime it is not clear which employers should be putting their efforts into working with and through what organisations. There is little point in enacting new legislation unless and until we take action to address the current skills crisis, both by organising greatly improved co-operation between public and private sectors (see the EURIM submission to the Police Reform White Paper⁴ and by addressing the development, assessment, and accreditation of the skills needed on the scale needed.

2) Summary of Key Points and Recommendations

- Crimes involving ICT systems are now commonplace and are beginning to threaten the integrity of our national prosperity.
- Skilled resources available to law enforcement are inadequate for the scale of the task, both in numbers and in training. Both priorities and responsibilities for action need review:
 - o Training in this critical sector is not measured against any national benchmark;
 - o Skills and competencies are not assessed against any national framework;
 - o No single Department claims responsibility for policy or delivery in this area;
 - o There are several executive agencies, including sector skills councils, with responsibility overlaps and gaps, but no lead agency.
- **A lead Department for policy and delivery must be agreed as a matter of urgency.**
- **The new Criminal Justice Sector Skills Council –Skills for Justice - should be given the task of sorting the current confusion of bodies and agencies with responsibilities for specifying, delivering and assessing the skills needed.**

3) The Nature of the Problem

Crimes involving ICT systems are now common-place and information in digital form may need to be handled in a wide variety of crimes even where computers are neither the target of attack nor one of the primary tools used 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 volume and complexity of such evidence places greater burdens on the resources required to undertake investigations – billions of characters of data are being seized in a single case.

4) Certification, Accreditation and Qualifications in the Criminal Justice Sector

It is appropriate at this point to define some of the key terminology used in this report::
Accreditation refers to the procedure by which an authoritative body gives formal recognition that a body or person is competent to carry out specific tasks. UKAS is the sole national accreditation body recognised by government to assess against internationally agreed standards, organisations that certify the competence of individuals or certify services such as the provision of training.
Certification refers to a) all the activities by which a body accredited by UKAS establishes that a person fulfils (and re-demonstrates at regular intervals) specified competence requirements and b) the process by which a body accredited by UKAS certifies that training provision (including the course content) fulfils specific requirements in terms of quality and suitability for purpose.

³ PSSO Skills Foresight Steering Group report, Section 5.5.9, published by the Skills for Justice Sector Skills Council in April, 2004

⁴ <http://www.eurim.org/briefings/resptochoconsr2.htm>

Competence is the demonstrated ability to apply knowledge and/or skills and, where relevant, demonstrated defined personal attributes.

Qualification is internationally defined as the demonstration of personal attributes, education, training and/or work experience. In the UK, the term is generally used to mean the result of demonstrating a level of knowledge attained through attendance at a formal course or equivalent.

There are currently no widely recognised qualifications for investigators, computer forensic experts and the like. If there is to be trust and sharing between people with these skills across the public and private sectors, and possibly internationally, there would be real benefit in having qualifications that are commonly acknowledged. A balance needs to be struck between formal qualifications, which take time to define and to introduce and may be a long-term goal, and the need for measures to encourage mutual trust and recognise competence to present evidence in the short term. This report focuses on attainable short-term objectives - the long-term issues are addressed in the current DTI Foresight project: *Cyber Trust and Crime Prevention*.

There is a need to distinguish between **accredited certification of training provision** (including fitness for purpose of course content) that results in a recognised and publicly accepted qualification and the **accredited certification of individuals** who have demonstrated a specific level of competence and/or knowledge. Accreditation is essential if there is to be universal acceptance of the quality of training and certificates and only with formal accreditation are qualifications likely to be seen as having worth. Accredited certification can also ensure that standards, once achieved, are maintained. Equally, some qualifications will require robust updating (eg: continuous professional development) programmes to ensure those with the qualification maintain their knowledge and skills over time.

Agreement to definitions of competencies will be a key contributor to the work on accreditation and accredited certification since that process requires criteria that can be used in the certification process for individuals, and the accredited certification process for providers.

5) ICT Courses and Training in the Criminal Justice Sector

While there is some investment in courses in particular skills for law enforcement agencies, and there are commercial trainers and academic institutions running courses in similar skills for industry, there are currently no widely recognised computer-related qualifications for a wide range of people across the criminal justice system, including 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 *also* internationally, there would be real benefit in having accredited certifications that are universally acknowledged. There are moves in this direction with organisations such as the Institute for Communications Arbitration and Forensics (ICAF) and the Council for the Registration of Forensic Practitioners (CRFP), 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 relative levels of this training are not assessed, content can be specific to the target audience and there is currently little contact between the various training providers in this area. The achievements of existing training providers are impressive, given the resources currently available but without a properly funded national skills framework these are at risk. An employer-led, coordinated exercise in this area could yield rapid results.

Recommendation a: - Potential Quick Win

BCS, C&G, IMIS, OCR, Sector Skills Councils, et al, urgently to review their existing end-user and technician qualifications and ensure that they not only include practical and up-to-date content with regard to security but that this forms a mandatory part of the practice and assessment routines.

An immediate task is to rationalise the confusing jungle of courses and training providers (and thus “qualifications”). A similar tangle of “clubs” is cited by court witnesses to bolster their claims to expertise. (The actual creation of a national framework for such training is clearly essential but is a longer term task, not a quick win.)

⁵ <http://www.iee.org/Policy/Areas/it/cyber/index.cfm>

Recommendation b: - Potential Quick Win

Build and populate a simple table to illustrate how those who develop and pay for relevant courses, materials and qualifications relate to each other. Entries might include:

- *Government Agencies and Accreditation/Certification "Authorities" with roles in this area: e.g. skills councils, curriculum and qualification bodies, professional institutions.*
- *Course and Qualifications developers (sectoral, professional, not-for-profit or commercial) with relevant exams, certifications, CPD programmes or registration programmes .*
- *Current delivery providers (and their relevant roles, qualifications, programmes and areas of expertise).*

Recommendation c: - Potential Quick Win

That a co-ordinating group be set up with representation from the key public and private sector agencies (e.g. Centrex, ICAF, Skills Councils and the Universities and commercial training providers most active in this area) to agree common approaches to the accredited certification of training for ICT investigators and forensics experts.

6) ICT Forensic and Investigatory Skills and Competences

There is a need to certify that an individual not only has the requisite knowledge, but also is competent (ie: has the ability, experience and integrity to apply that knowledge effectively). Industry and law enforcement need similar skills to tackle effectively crimes involving computers and the Internet, yet there is no commonly agreed definition of the sets of competencies, knowledge and associated skills that cover investigations and forensics. It is unlikely that a universal set of job definitions can be identified, but lists of overlapping knowledge and skills could be created that can be combined to describe particular types of task for which individuals are qualified. There are a number of potential sources for such definitions. For example, NSLEC has established a set of competencies that underpin their courses and a suitable framework exists in the form of the Skills Framework for the Information Age (SFIA)⁶. Common to all such considerations, is the need for quality controlled Continuing Professional Development programmes that record and assess the ongoing experience and competence of individuals.

It is not clear what remit the new Sector Skills Councils will have in this area or how they will contribute. Common understanding of the required sets of skills, sharing of the costs of creating and providing appropriate training and recognition of commonly accepted accreditation and certification processes could cut costs and encourage sharing of resources and information between the different constituencies. There is at present no national framework of qualification or certification that might allow, for example, the relative worth or integrity of an outside contractor to be judged. The private sector has a key role to play in addressing this lack, but can do so effectively only if a national framework is in place. That framework should be embedded into the wider, employer driven sector skills structure Government has implemented, but there appear to be at least five current or planned sector skills councils with remits relevant to parts of the e-Crime Agenda:

- Skills for Justice - taking over from the Police Skills and Standards Organisation and the various bodies concerned with all parts of the public sector side of the Criminal Justice systems, including CPS, Prison Service et al.
- Security - which covers the private sector side of prevention, investigation and detection.
- E-Skills - which covers information systems development, service and user skills with regard to computing and communications.

⁶ <http://www.sfia.org.uk/cgi-bin/wms.pl/296>. SFIA maps areas of work on one axis and levels of responsibility on the other. It can be adapted to the training and development needs of a very wide range of businesses and includes skills audit, planning future skill requirements, development programmes, standardisation of job titles and functions, and resource allocation. Jointly "owned" by BCS, IMIS, IEE and e-Skills, it offers a practical tool for assessment and certification in this area.

The EURIM e-Crime Home Page is currently at: http://www.eurim.org.uk/activities/ecrime/e_crime.htm

- SEMTA - which covers science and engineering, including the manufacture of computing and communications equipment.
- Skillset - which covers multi-media skills, including the image processing and manipulation which is forming an increasing part of modern digital evidence.

As yet, Skills for Justice has no specific remit in the area of computer-assisted crime and its business plan does not make provision for appropriately-trained resources. e-Skills has expertise across the more general ICT spectrum. The over-arching body, the Sector Skills Development Agency (SSDA) has been established to underpin the SSC network and promote effective working between sectors. Its “golden theme” is to establish a lead body in areas where there is an overlap. It would therefore seem appropriate for Skills for Justice to be encouraged by SSDA to assume the lead and include the need to address e-crime skills as part of its business plan, subcontracting to, or otherwise supported by the others. e-Skills, for example, would then define the skill-sets in a SFIA context. The over-riding consideration must, however, be that the strategy is driven by the needs of the relevant employers.

Recommendation d: - Potential Quick Win

That Skills for Justice be tasked by SSDA as the lead agency in the future development of frameworks and specifications for training, and certification of appropriate skills across all communities and that e-Skills be encouraged to support, within a SFIA framework as and when appropriate

Recommendation e:

Encourage industry-led certification schemes, perhaps based on existing qualifications, such as that provided by CFFC Shrivenham, combined with a Criminal Records Bureau search to cover the skills appropriate for advising enterprises.

The products, services and networks which need to be understood by those involved in the fight against e-crime often involve international co-operation.

Recommendation f:

Progress debate on how the relevant English and Welsh skills frameworks fit into those being developed for Scotland and Northern Ireland, as well as those at European and International levels.

Recommendation g: - Potential Quick Win

That an informal group be set up under the lead of Skills for Justice, with representation from key users and providers of expertise, to collate the specifications already available in a common framework of definitions of competencies and skills for ICT investigators and experts in forensics.

7) The Need for General Awareness

Part of any solution aimed at matching the availability of adequately trained resources in the public sector with the incidence of computer-assisted crime is the need to raise awareness, at the lowest levels, of the risks. The EURIM-IPPR paper: *Protecting the Vulnerable* analyses this challenge in relation to the citizen and to the SME and makes recommendations. These need to be progressed since “general awareness” appears to be below the threshold for public sector support and the most comprehensive guidance is currently that on the ICAF⁷ and IEE sites⁸.

8) Resources, Priorities and Government Funding

Law enforcement does not have, and is unlikely to have in the foreseeable future, the capacity to handle the majority of reported incidents. 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 large volumes of data to be sifted.

This lack of resource makes it imperative that a lead Department, such as the Home Office as sponsoring Department for Skills for Justice, is identified as having responsibility for coordinating relevant cross-departmental funding (including related to investigatory powers and crime-related health and safety) to facilitate the aggregation and allocation of the relevant public sector budgets to support accreditation and qualifications, courses and materials to meet common needs, in partnership

⁷ http://www.theicaf.com/accounts/ICAF/documents/Dec2003/ECS_WP3_adobe_031116.pdf

⁸ http://www.iee.org/Policy/Areas/it/security/NHTCU_version.pdf

with the private sector, both as employers of security staff and as providers of training and contractors.

In the international context, e-crime has strong cross-border characteristics and international law-enforcement bodies have already produced guidance to assist cross-border co-operation. Given that most cross-border investigations entail close co-operation with financial and communications service providers, that guidance needs to be shared with relevant private sector partners, in the same way that the relevant ACPO guidelines have been made available in the UK. Formal publication (appropriately sanitised) would greatly assist “commonality of approach” in training to handle cross-border, cross public/private sector investigations. For example, elements of the Interpol Manual, although part of a restricted law enforcement document with concomitant restricted circulation, might, with Home Office and NCIS blessing, be declassified and distributed with advantage to private sector partners.

Recommendation h:

That the Home Office works with and through Skills for Justice and Professional Institutions to mandate the inclusion of practical ICT security in all publicly funded end-user and technician training

Recommendation i:

That the Home Office assumes lead funding responsibility for the e-crime element of the work of Skills for Justice and that Skills for Justice be made responsible for progressing investigatory training standards (including those required under RIPA) and all other Departmental investigatory and computer forensics training standards, together with similar training standards for the private sector

Recommendation j:

That the Home Office champions the cause of cross-border public/private partnership cooperation in the gathering, custody and presentation of digital evidence and takes a lead, including funding as necessary, in editing relevant material (e.g. the Interpol Manual) for shared use with relevant private sector partners.