



Policing: Building Safer On-line Communities Together **EURIM response to the Home Office Police Reform White Paper**

Introduction

EURIM is an all-party parliament industry group concerned with the politics of the Information Society. It has over a hundred parliamentary members (including Ministers and Front Bench Spokesmen) and over seventy corporate and associate members as well as over a hundred observers from Government Departments and the Public Sector. Because of the timescale it has not been possible to go through our normal membership consultation. This response is based on the work of the team working on the EURIM - IPPR study to help set the agenda for a national strategy for addressing E-Crime.

The response is structured with an initial preamble, which gives the background to the response, followed by a summary of key points. There are two supporting appendices. One is the discussion paper launched in December, summarising the conclusions from the first phase of the EURIM - IPPR Study. The other is the report of a workshop to discuss possible responses to paragraphs 4.19 - 4.21 of the consultation paper. As will be clear from that report, we have only "scratched the surface" of the issues that will need to be addressed and would be pleased to help with more detailed consideration of the options.

Preamble

The forward to the consultation refers to the need to "empower local communities to engage in the common endeavour of beating crime". More than half the population of the UK are now regular users of the Internet, as is over 10% of the population of the world. So too is a similar proportion of criminals. The criminals are using the technology to commit old crimes more efficiently and to commit new ones. At the Crime Science conference organised by the Jill Dando Institute in November 2003 over 200 delegates, mainly from law enforcement, were told by Nick Ross (Crimewatch) how traditional crime broadly splits into:

- opportunistic crime - committed by those who are lazy or mischievous - which can be greatly reduced by the simple precautions, visible deterrence, the fear of detection and the application of scientific method to designing out vulnerabilities
- and
- organised crime - committed by those for whom it is a business and who are often in advance of law enforcement in the application of technology - this is far harder to deter and commonly requires intelligence led policing to unravel and address

In the electronic world we can see a similar pattern emerging and the result threatens to overwhelm the ability of law enforcement to cope.

The Internet has been described as "The Wild West without six guns". But the involvement of organised crime means that many of those behind the current wave of denial of service attacks (the on-line equivalent of traditional extortion rackets) and "phishing" expeditions (some precisely targeted, others mass-market) are deploying very much more effective tools than the six-gun to achieve their objectives. Meanwhile the investigatory backlog mounts.

The Wild West was tamed by Pinkerton Men and Vigilantes because traditional law enforcement could not cope. If we wish to preserve our traditions of democratically accountable policing we need to move rapidly to ensure that UK law enforcement can.

But the current disparity between the electronic security and investigations budgets of law enforcement and of industry is even greater than that during the decade of so after the American Civil War between those of the Sheriffs and Deputies and of the Banks and Railroad Companies. The total funding available to the NHTCU (including for supporting Computer Crime Units) is less than the individual electronic security and investigation budgets of most major High Street banks or of the main network or outsource suppliers.

Meanwhile, if more funding was to be made available for public law enforcement there is a widespread impression that the majority of voters would prefer to see it spent "putting bobbies on the beat, not skulking in offices behind computer screens". The exception is with regard to the apparently rising tide of paedophile activity over the Internet, linked in the public mind with the pornographic spam supposedly filling the e-mailboxes of their children and grandchildren, even if the parents and grandparents are not themselves on-line to see it.

In this area there may be strong support for a change of scale in the resources deployed by law enforcement to actively investigate and prosecute more of that which is already reported, as well as to remove barriers to what suppliers can do to protect their customers, including parents and children as well as small firms, primary schools, play-groups, study centres, after school clubs and other "businesses" with little or no budget for ICT, let alone security, support.

This raises issues of skills and governance which will require inter-departmental co-operation, not just with DTI and DfES but also all those departments, agencies and regulators with investigatory powers or at risk from computer assisted fraud. The solutions will also require funding. There is a clear desire to reduce the cost by involving volunteers but, even if this is successful, most will have some but not all of the skills and experience required and will need training. Even those who do not need training will need basic vetting. They may also need more advanced vetting if their skills are to be most effectively used.

The first appendix to this submission concludes that we need a major consultation exercise "structured in such a way as to bring the necessary players together, across organisational boundaries, to identify and recommend solutions that will work". Such an exercise will need serious funding but will cost far less than ineffective, or perhaps even counter-productive, policy. It also needs to be joint, across departmental boundaries, as with the "21st Century Skills" consultation, led by DfES but signed off by the Prime Minister, Chancellor and three Secretaries of State.

The second appendix to this submission focuses on the some of issues that will need to be addressed if we are indeed to harness industry and voluntary resources in support of law enforcement in the fight against computer-assisted crime.

EURIM would be pleased to help organise practical follow up in both areas.

Summary of Key Points relating to Specialist Constables (4.19 - 21), Civilian Volunteers (4.22) and Lead Forces (6.10)

ICT has long been a career for those who are mentally but not necessarily physically able. More-over few of the experienced ICT professionals who volunteer to assist programmes such as IT4Communities are aged under 50. Current UK police frameworks allow for the employment of the disabled and over 55s as part-time professionals but not for their use as volunteers. While it is possible to make recommendations within existing legal frameworks, there is a need to consider whether some of the constraints are really necessary.

If the shopping mall, housing or children's playground would benefit from a "Community Support Officer" with limited powers, acting as a visible deterrent and as the eyes and ears of law enforcement, capable of acting as a professional witness, would not a similar approach be appropriate for Internet auction sites, discussion groups and chat rooms? And does the "virtual community support officer" need to be physically able to walk, let alone run.

Each year, several thousand women ICT professionals leave the ICT industry because they cannot combine the employment opportunities on offer with the need to fund care for their children or, increasingly, for elderly relatives. Over the past three years, somewhere over

100,000 men have also left the ICT industry as jobs have been lost or moved overseas. The market has (most recent quarter) shown a modest upturn but many individuals have neither the skills in current demand nor the opportunity to acquire or demonstrate them other than by undertaking semi-voluntary roles providing computer support to schools or charities.

Meanwhile the UK currently has seven industry-funded professionals and a couple of dozen specialist police officers to address a child protection task for which the United States had (two years ago) trained over 600 “silver surfers” (drawn from the pensioners of both law enforcement and the ICT industry and funded by the latter) and is currently said to deploy over 400 FBI officers handling the investigations they have helped launch.

A number of the models used in other countries do not fit with the current UK policing environment and there are concerns over political and social acceptability, as well as legal and administrative practicality. However, there is growing pressure for action. More-over industry, especially financial services, is bearing the cost when similar “grooming”, alias “social engineering”, techniques are used to inveigle account information and personal details from mature customers to bypass electronic security. Their losses and the tax revenues lost to the exchequer, may already be considerably greater the cost of effective action.

This will not be any easy area to address. The moment one moves outside current UK frameworks, deficient though they may be, there is a need to address issues of governance and liability, let alone responsibility for the costs of vetting and training. There is also the equity and practicality of expecting one individual to do for free that for which another might charge £100 an hour (or more) given the shortage of specialist skills in some areas.

The participants in the EURIM-IPPR study therefore recommend a step by step approach: beginning with that which can be done within existing legal and administrative frameworks, then making extensions for which there is widespread support while, in parallel, consulting thoroughly on those recommendations which entail major change.

The first steps should include pilots to test the practicality of:

registers of experts on whom law enforcement can call for technical assistance under existing governance arrangements. The organisation, promotion and administration of such registers is a non-trivial task and will need funding, including for vetting and updating arrangements. There are also issues of liability, including for experts “volunteered” by their employer to provide support which might or might not be professionally charged.

routines for Internet special constables akin to those now being piloted for fraud specialists. These might initially be promoted among those experts with whom police will wish to share operational information or who may be asked to assist with the gathering and analysis of evidence, as opposed to “merely” helping with technical support. It should, however, be noted that success will be limited until some of the deficiencies in the current model have been addressed because many of the industry security experts most likely to volunteer would find it difficult to meet current physical fitness requirements.

multi-disciplinary Internet Crime units, staffed jointly by secondees from law enforcement and from industry, akin to those addressing card and payment fraud, to address specific types of Internet Crime (e.g grooming, phishing, denial of service linked to extortion). The success of the existing units raises, however, many questions, including of funding, accountability and priority setting. These need to be openly discussed and possible solutions tested.

We also need to ensure that the **business plans for the Criminal Justice Sector Skills Council include the means of developing, assessing, accrediting the addressing investigatory and forensic skills needed**, not only for full-time law enforcement professionals and support staff but also for registers of experts to function, for specialist constables and civilian volunteers to be assessed and trained, for multi-disciplinary teams to become effective rapidly and cost-effectively and for industry-law enforcement co-operation, including spreading the cost of good quality course and materials.

In parallel we need to explore the potential for greatly enlarging the pool of volunteers available, but under governance routines that are acceptable to all concerned, including the Courts.

We also need to look at the use of part-time professionals, perhaps on terms akin to those for interpreters or police surgeons.

Among the areas which might be explored are:

limited warrant special constables, so as to make more effective use of industry security professionals who are not physically fit to perform the traditional duties of a constable or who may have constraints on their availability or suitability (including for commercial reasons)

virtual community support officers whether or not they are full-time, paid or physically fit: perhaps with special arrangements to attract women returners, computer science students, silver surfers and other such groups to help with monitoring chat rooms and some of the more labour intensive track and trace tasks that are currently not being addressed at all for lack of resource.

international investigation teams: those multinationals with operations around the world (banks, oil companies, airlines and ICT infra-structure suppliers) often have more experience of handling cross-border attacks and threats than most law enforcement agencies but the means of tapping that expertise appears very limited.

Once again, however, it is suggested that the need is to begin with monitored pilots to build confidence.

The attached appendices cover some of the thinking behind the above in more detail, particularly the creation of registers of volunteers. Those concerned would be pleased to help explore these ideas further, including perhaps with the organisation of pilots.



THE EUROPEAN
INFORMATION
SOCIETY GROUP

EURIM



Partnership Policing for the Information Society

Separating myth from reality and snake-oil from practicality

Identity theft is replacing drug trafficking as the crime of choice

Drug gangs move in on fake £1.3 billion trade -

The Times 18 August 2003

Every day Scotland Yard's paedophile unit deals with images of the most harrowing nature ...

Oh, my God, what am I looking at? -

Daily Telegraph 31 August 2003

The Internet payment system Worldpay is under attack from unknown assailants, hitting thousands of online retailers worldwide

Worldpay battling online attack –

BBC News 5 November 03

E-crime¹ is becoming a topic of mainstream news. Contrary to popular perception, most of it is familiar crime – fraud, pornography, impersonation, etc – exploiting the new on-line world.

1. Why does the subject need political attention - NOW?

Around half the population of the UK has used the Internet. Over a quarter now use it regularly. So, almost certainly, do a similar proportion of criminals, whether to organise traditional crimes more efficiently or to commit new ones. The UK Government has an objective to make Britain the best place for Electronic Business and the Home Office has announced that it intends to publish a cross-cutting strategy to address E-Crime next spring. But as yet the debate on e-crime to which the Government will need to respond is a mixture of hysteria and denial. Either the issues are earth-shattering and demand action or they are trivial and can be handled by a little user-education. Finding the middle ground will require a constructive debate that is so far missing.

This is the first paper in a series to promote that debate. It summarises the issues addressed in a series of supporting working papers. The supporting papers contain specific recommendations as to how government, industry and society can work together to improve the situation, including some “quick wins” to give early benefit at low cost, as well as confidence that those “in charge” (whether in industry or government) know what they are doing and can be trusted to deliver.

Overall success will, however, depend on action in three key areas:

1. The development of a shared **National E-Crime Strategy** for achieving a safe information society that involves and is supported by all constituencies across government, industry and society.
2. Government and industry support for **co-operative research and consultation** on the actions necessary (including information assurance, security, education and other forms of prevention) to address the risk and fear of e-crime.
3. Developing **the capability of law enforcement** (including routines for co-operation with industry) to identify and deal with threats as they emerge (rather than reacting when they are out of control and thus very much more difficult to contain)

¹ Defined here as “crime that requires ICT expertise during investigation”.

2. The Political Framework for a National Strategy

The Emerging Perception of E-crime

Over the past year the threats from e-crime have moved from being of concern to industry specialists to being a topic of mainstream news. Below is a selection from the headlines and articles in the national media during the summer and autumn of 2003. Together, they inform and inflame public opinion and ensure this will become a matter for political debate during the run-up to the next general election, if not before.

<i>More than 7 million people in America have been the victims of identity theft</i>	Identity theft explodes in US - BBC 21 July 2003
<i>The SOBIG F virus has set records for the amount of e-mail messages it infected</i>	SOBIG is biggest virus of all - BBC 21 August 2003
<i>High tech security investigators and police were involved in a global race against time last night to find 20 home computers harbouring a programme that threatened to cripple the Internet</i>	Global hunt to kill off Internet Virus - Daily Telegraph 23 August 2003
<i>The trials of thousands of alleged paedophiles accused of buying pornography on the Internet are in jeopardy</i>	Porn case delay after computer trial collapses - The Times 23 August 2003
<i>New and more dangerous computer viruses are growing at such a rate that the whole Internet could collapse</i>	How firms can suffer even from preventing a virus - The Times 23 August 2003
<i>A computer expert masterminded Britain's biggest credit card fraud ...</i>	Fraudsters duplicated 9,000 credit cards - The Times 6 September 2003
<i>Barclays has called in the cyberpolice and slapped a limit on online cash transfers in an attempt to head off an e-mail fraud aimed at Internet banking customers</i>	Barclays calls in cyberpolice - Guardian 15 September 2003
<i>Computer giant MSN is closing all its Internet chatrooms - to stop perverts using them to prey on children (this Sun "exclusive" was also on the front page of the Guardian, Independent, Mail, Telegraph, Times and Financial Times as well as radio and TV news and all the wire services).</i>	Microsoft chatroom shutdown over pervs - Sun 24 September 2003
<i>Busiest US port hit after Dorset teenager allegedly launched electronic sabotage against chatroom user.</i>	Hacker left port in chaos - Guardian 7 October 2003

There were many fewer headlines putting the contrary view although these are said, by industry experts, to be more realistic:

<i>In every day life, with a few simple precautions you can keep your personal details private</i>	The leaky net - BBC 29 July 2003
<i>The latest e-mail virus may be the worst ever, but experts argue that its actual economic impact is likely to be modest</i>	Modest cost of SOBIG virus - BBC 22 August 2003
<i>Banking is cyberspace is quicker and easier ... a few simple precautions ... we have overcome our fear ...</i>	The high street is given a powder - The Times 20 September 2003

Constructive debate requires both industry and government to recognise the reality of public fears at the same time as ensuring that all concerned do what is practical now, without waiting for GODOT (the next Generation Of Digital Operating Technologies), let alone the resolution of cross-border jurisdictional problems which date back to the days of tramp steamers and gunboat diplomacy. E-crime is not a problem for tomorrow - it is a challenge for today.

In the physical world shoppers like clean, well lit and well policed shopping malls. They avoid streets with graffiti, broken glass and boarded up shops. It is much the same in the electronic world, except that the scale and immediacy of the problem, together with the social and economic impact, are not local, they are international. The need is to enable citizens and business to enjoy the same level of protection and confidence on-line as in the physical world.

Enabling a Safe and Trusted Information Society

Society is becoming increasingly dependent on computers and the Internet. Government has set an objective to make the UK the best place to do business electronically. Challenging targets have also been set to involve business and citizens in communicating with government electronically. The private and voluntary sectors are routinely exploiting the electronic world. Citizens increasingly use computers and the Internet for a wide range of social, educational and other purposes. Always-on connection via broadband is being encouraged to accelerate this exploitation of the digital world for business and for pleasure. The continued success of these moves to the digital age is critically dependent on the perception that they are safe. Neither government nor business will achieve their goals if any substantial part of society comes seriously to doubt that safety.

A first step is to update policing frameworks for the electronic world. Government has recognised this by introducing new or revised legislation, such as the Regulation of Investigatory Powers Act, to help address specific areas of concern to law enforcement. Such legislation, however, addresses only part of the problem and can, if misconceived, even be counterproductive. This technology permeates society in ways that require new attitudes and approaches to create structures within which government, industry and law enforcement can co-operate in establishing safe and trusted environments in which each plays its agreed part.

We need to focus on partnerships of equals to ensure that the services being put on-line by government, industry, education and the voluntary sector are both trustworthy and trusted. We need to identify those who should contribute to such partnerships and to involve them actively in developing the solutions needed.

The Balance of Priorities

There is already significant debate on the relative priorities for law enforcement given that their resources are limited. Current priorities are focused on visible social issues, such as street crime, burglary and car theft on the one hand, and on 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, leading industry to take greater responsibility for the investigation and prosecution of some offences. Examples include the actions by the software and entertainment industries to combat piracy and illegal copying and by the financial services industry to combat card fraud. Industry and the voluntary sector are also taking the initiative to encourage reporting of, and action against, unacceptable activities in specific areas - notably relating to the protection of children - with, for example, the setting up of the Internet Watch Foundation.

As yet, e-crime is seen (correctly or otherwise) to be a minority concern. However, increasing publicity on the extent to which the new technologies are being exploited to support criminal and anti-social activities is beginning to cause people and organisations to question how they can defend themselves. Whether or when this will result in widespread public demand for action is uncertain, but there is a need to have effective policies and action plans ready for implementation when it occurs.

The current National Policing Plan does not explicitly include activities relating to e-crime. Local police forces therefore have no incentive to devote resource to this activity, because it does not contribute directly to the achievement of performance indicators set by government. Local computer crime units in most police forces are inadequately funded, have critical backlogs of investigations outstanding and are unable to undertake any proactive investigation. That situation will not change unless and until public awareness and political pressure lead to a change of priorities. Such pressure will imply, however, that the medium is indeed felt to be unsafe. Meanwhile, industry and government will not be able to respond with comparatively modest effort unless the groundwork for effective partnership is already in place and working.

Many of the recommendations in this paper are therefore based on a perception that industry will have to take the lead in developing the necessary capabilities to combat e-crime in order to compensate for its low ranking among current priorities for law enforcement resource.

3. Challenges and Questions

To date the focus of debate has been on combating e-crime - with varying definitions as to what is meant by e-crime. For example a recent book² on e-commerce crime contains a seven page list of types of e-crimes with examples of each³. For the purposes of this Study three broad categories of activity are addressed:

- 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).

Policing and law enforcement, supported by legislation, are taking time to adapt to these new threats, often beginning with misguided attempts to control the technology through lack of understanding as to how it is used or how it works in the real world⁴. Use of new technologies is expanding and changing in ways that makes this approach inadequate. Small firms and individual citizens are seeking to use technologies that were previously the province of experts. Large firms are seeking to address mass markets from global centres as opposed to local subsidiaries. Technologies previously available only to experts are now available to most teenagers. The widespread adoption of broadband (always on) connections increases vulnerability to attack and misuse. In consequence some problems are growing exponentially.

There is, however, also evidence that the use of these new services is inhibited by concerns over safety and trust. The latest ONS Internet access survey shows that, of those people who had never purchased over the Internet, 23% cited security concerns as the reason. 9% of those who don't use the Internet cite security concerns. Polls suggest that 40% of those who currently do not use Internet banking would do so if their fears over security could be resolved and that among web users only 25% had no worries about buying goods and services online.

As in the real world, if people perceive they are vulnerable they will avoid putting themselves at risk: just as they will avoid some inner city areas by day, let alone by night - thus reinforcing a cycle of decline. There is a real threat that perceptions of the Internet as a dangerous place will, at best, inhibit growth and, at worst, destroy trust in electronic services. A pro-active approach is required that creates the right balance of trust and caution: the electronic equivalent of not walking down a dark alley at night and not leaving purse or wallet unattended on the counter when you turn away. This approach needs to involve skills and resources from many constituencies in the creation of safe environments where opportunities for criminal activity are reduced, people feel at least as safe as in the high street or park and business is confident in offering on-line services.

This will require a common understanding of the capabilities and concerns of each constituency, as well as their roles and responsibilities in creating a safe information society. Parents, large commercial organisations and law enforcement have very different worries and concerns and very different capacities to address them. We need to engage all involved parties across the public and private sectors in an open debate to agree priorities and frameworks for co-operation, making best use of the limited resources available. There is a need to identify how best to remove any barriers to effective partnership and how government can best help, remembering that trust takes time to establish, with

² *Superhighway Robbery: preventing e-commerce crime* by Newman & Clarke. Second volume in the Crime Science Series edited by Gloria Laycock, (formerly Head of the Home Office Police Research Group, now Director of the Jill Dando Institute of Crime Science, University College, London) Willanpublishing.co.uk 2003, ISBN 1-84392-018-2

³ Available as a supporting document [Scale and Nature of Computer Assisted Crime](#).

⁴ An example is the attempt by governments to control the spread of cryptography technology by classifying it as munitions. The widespread inclusion of advanced cryptographic technologies in commodity products for practical business purposes together with ready availability over the internet of the technology eventually forced governments to acknowledge that such control was not practical.

dialogue, example and experience more important than awareness campaigns or legislation, essential though these may be.

The questions for consultation include:

- How can we ensure and encourage global products and services that are less vulnerable to criminal exploitation but which respect the desires of those who wish to control their own systems and desire their private concerns to remain private?
- How should we educate and motivate users of all ages to be better electronic citizens, protecting themselves, looking after others and refraining from mischief or malice?
- How do we ensure that law enforcement is at least as sophisticated in its use of technology as those who are increasingly using computers and networks to help organise and commit crime?
- How should we police that part of cyberspace over which the UK might claim jurisdiction so that others will work with us when the location of the criminal is elsewhere or unknown?
- How do we ensure democratically acceptable and accountable frameworks for co-operation across boundaries, between law enforcement agencies in different jurisdictions and between public and private sectors, including both industry and interest groups?

Almost all the credible answers to these questions require Government, industry, law enforcement and education to work together - beginning now.

4. Areas for Action and Recommendations

In April 2002, EURIM called for a national strategy for tackling E-Crime (*Briefing 34: E-Crime – a New Opportunity for Partnership*). IPPR has called for action to protect the most vulnerable, (*Online Freedom and Safety for Children*, by Sonia Livingstone) including a surfing proficiency test for children. The Home Office has now committed to developing a cross-Departmental strategy, pulling together work in many areas covering e-crime. The current EURIM-IPPR Study focuses on six key areas where priority action is needed within that Strategy to reduce the impact of e-crime:

1. [Reporting Methods and Structures](#)
2. [Reducing Opportunities for E-crime](#)
3. [Addressing the particular needs of Small Firms and others who are most vulnerable](#)
4. [Roles & Procedures for Investigation](#)
5. [Growing the Necessary Skills](#)
6. [Legal Issues](#)

These have been explored in a series of workshops which produced the analysis and recommendations summarised below (full reports available on <http://www.eurim.org>).

Reporting Methods and Structures

There is a real lack of information on the extent to which e-crime is undermining trust in the information society. The first need is to improve and bring together existing work on reporting methods and structures. The second is to develop ways of handling the massive increase in volume were it to be made easier for business and individuals to report what is happening – probably by the controlled introduction of reporting mechanisms targeted for specific purposes. The final need is to improve the way intelligence on e-crime threats is gathered, analysed and disseminated to specific target audiences in the appropriate form.

Recommendations include:

- Government to build on the work of agencies such as PITO, NISCC, NHTCU and industry (including that of the Internet Crime Forum “One Stop Shop” sub-group) to encourage the development of seamless portals for the reporting of incidents and of websites to help people identify what types of problem they face and who they should contact for assistance.
- The relevant government agencies to work with each other and with appropriate industry organisations to provide better intelligence and reduce duplication of effort.

Reducing Opportunities for E-crime and Addressing the needs of the vulnerable

The need for crime prevention and to minimise the opportunities for criminals is familiar in the real world. In the emerging electronic world there is a need for similar approaches. This is hindered because most users have no practical basis upon which to judge risk in the digital world. There is, therefore, a danger that only technical or legislative solutions are considered even though, as with physical crime prevention, holistic approaches are essential for success in reducing opportunities for e-crime and promoting confidence in the comparative safety of the Internet. Such approaches also need to address both the perception and the reality of e-crime in very different communities. Those who use computers and the Internet without adequate security are not only a danger to themselves, they can also be a danger to the rest of an increasingly inter-connected on-line world. This has been shown by recent problems with the latest generation of viruses and worms, spread rapidly through poorly protected systems, as well as by “distributed denial of service attacks” using hi-jacked computers.

Waiting for a new generation of products and services to supposedly solve the problems is not an option. On the positive side, small business is targeted by many government initiatives, including those of DTI and DfES, albeit few of these have yet made significant impact on their attitudes and behaviour. There is a need for realistic advice and guidance tailored to the needs and concerns of small businesses and other vulnerable groups, widely disseminated through a variety of channels. This needs also to be supported by campaigns to encourage the provision of products and systems that default to secure settings and of trusted services that help those without ICT expertise to understand and implement risk management profiles appropriate to the usage they intend.

Recommendations include:

- Encourage hardware and software vendors, communications providers and ICT suppliers and retailers to work together to provide in their offerings ready-to-use security packages, installation and support services to help small firms better secure their systems at prices they are willing to pay, and that government mandate these for publicly procured equipment and services.
- Produce a “Green Cross Code” for the safe use of computers and the Internet in homes, schools and in small businesses, that could be distributed widely and that would provide advice, point to publicly available Codes of Practice and Guidance documents for further information, and explain what to do when an incident is suspected.
- Extend the syllabuses of end-user courses to address the basic security precautions that all PC and Internet users should take and teach good practice at all levels, from schools and colleges to workplaces and lifelong learning centres.
- Consider the WARP (Warning Advice and Reporting Point)⁵ approach developed by NISCC as the model for a broader scheme to encourage local sharing of incidents, information and intelligence within and between communities.

Roles and Procedures for Investigation

Many conventional crimes now involve the use of ICT systems. Consequently evidence in digital form offers new investigative opportunities even where a computer is neither the target of attack nor the primary tool to commit the crime. New skills and techniques 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 ensure the provenance of evidence in digital form. The ability of law enforcement to cope is further impacted by the significant extra cost of investigations that involve digital evidence. Finally, 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.

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. Better ways of encouraging sharing of expert resource between industry and law enforcement are needed to alleviate these constraints.

⁵ Warning, Advice and Reporting Point

Recommendations include:

- The Home Office, DTI, law enforcement and relevant trade associations and professional bodies to co-operate in developing and publicising good practice Guidelines⁶, Standards and Codes of Practice for e-crime investigations, and to investigate the practicality of accrediting investigators and others in industry with appropriate skills and experience to work to the same legal standards and guidelines as law enforcement agencies when investigating e-crime.
- Home Office to co-ordinate work with all interested parties to create processes that can be understood and used by any organisation or individual to verify the provenance of requests for access to or retention of data in electronic form (not just communications data) or for specialist ICT support by any authorised investigating body.

Growing the Necessary Skills

Significant investment is already being made in creating and running courses in particular skills for law enforcement agencies. There are commercial training operations and academic institutions running courses in similar skills for industry. There appears to be little, if any, linkage between many of the groups looking at the issues of competence and probity or involved in training. It is not clear what remit the new Skills Councils will have in this area. There is currently little contact between the various skills providers in this area, nor is there any common agreement on the sets of skills (particularly those at the higher levels) for which training would be most beneficial. Common understanding of the required sets of skills and sharing of the costs of creating and providing appropriate training could cut costs and also encourage further sharing of resources and information between the different constituencies.

Recommendations include:

- To create a co-ordinating group with representation from the key public and private sector agencies to agree skills and training priorities and the potential for sharing resources and materials
- The Learning and Skills Councils and other DfES funding agencies, working through the relevant bodies, to mandate the inclusion of practical security in all publicly funded ICT end-user and technician training.
- Government agencies to encourage simple industry-led voluntary accreditation schemes, within relevant UK and International frameworks, to cover those offering information security consultancy, advice and skills, including those appropriate for supporting SMEs.

Legal Issues

The Computer Misuse Act (CMA) has been around since before the widespread use of the Internet and is perceived to be in need of updating. Reviews have concluded that only minor changes are needed to maintain its perceived and actual effectiveness and that these should be urgently incorporated. Some conventional crimes (e.g. theft, impersonation) are legally defined in ways that make prosecution in the intangible world difficult or impossible. The need is for changes to the relevant laws to make the commission of an offence independent of the means - i.e. technology neutral. The Law Commission has carried out a number of studies to identify priority areas where such changes are required. Introducing these changes would significantly increase confidence in electronic business and enable a wider range of computer-enabled criminal activities to be successfully prosecuted and punished.

A major need is for more effective co-operation across jurisdictional boundaries. The harmonisation of penalties with regard to specific computer-related crimes such as denial of service and hacking across EU member states may help but it deals with only a small part of the problem. Cross-border investigations can be greatly facilitated by the G8 24/7 contact process and effective mutual assistance arrangements.

Recommendations include:

- Government to initiate early and open consultation on the Law Commission recommendations on priority changes to existing laws to facilitate prosecution of e-crime, working with appropriate UK industry and law enforcement bodies to identify and implement those agreed to be of highest

⁶ The recently issued ACPO Good Practice Guide for Computer-based Electronic Evidence, available on www.nhtcu.org, is a good example.

importance as a matter of urgency.

- Home Office to agree and introduce rapidly amendments to the Computer Misuse Act to underpin its perceived effectiveness and to reinforce the message that e-crime is being taken seriously.
- Government should ensure there is early and continuous industry input in international forums discussing the development of global (including pan-European) co-operation on proposals and legislation addressing the fight against e-crime to ensure that they are effective, practical and, as far as possible, technically neutral

Consultation

The recommendations in these papers can be achieved only if effective consultation processes are in place. EURIM has produced two studies on consultation processes: Briefing 26 in May 1999, [*Consultation, Concealment or Confusion: Practices and Principles for European Policy Formation*](#), and Briefing 30 in July 2001, [*Making a Reality of Consultation*](#). These recommend that effective consultation involves all interested parties in government, industry and society at large, is properly funded and is part of an open dialogue on the proposals under review.

At a high level the issues to be addressed are relatively simple. People and organisations need to understand better how to manage their systems to address risks in the intangible world. Systems and services need to be made more resistant to accidental or deliberate misuse. Products need to be made simpler to install and to configure to minimise risk.

Unfortunately, achieving these simple objectives is complex, involving co-operation across many Government Departments and industry bodies and will require significant long-term commitment from key players. While there appears to be consensus on the detailed recommendations in the supporting papers produced in the course of this study, the means for establishing coherence across the implementation of those recommendations (so a that consistent image is perceived by those on the receiving end) is less than obvious.

The consultations, therefore, also need to be structured in such a way as to bring the necessary players together, across organisational boundaries, to identify and recommend solutions that will work.

© 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.

APPENDIX 2



Summary Report of the meeting of the EURIM-IPPR E-Crime study group on possible EURIM response to the Police Reform White Paper, held on 15 January 2004 in Room C, 1300-1500, 1 Parliament Street, Westminster

Chair: Philip Virgo (EURIM)
Rapporteur: Dave Wright (EURIM)

1. Introduction

1.1 Philip Virgo as Chair opened the meeting, stating that the objective was to help produce a submission to the Police Reform White Paper especially sections 4.19 - 22 and 6.10 calling for inputs on Specialist Constables, Civilian Volunteers and Lead Units.

1.2 Working Paper 4, Roles and Procedures, of the EURIM - IPPR study had found that law enforcement was unlikely ever to have the capacity to handle all potential incidents if they were reported. It would therefore reduce the load on law enforcement if investigations in the private sector could be carried out by people accredited and 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.

1.3 At the very beginning of the EURIM - IPPR study the idea of Specialist Constables was floated, but there were concerns over whether the Special Constable role was the right model. Different situations might require different types of co-operation and governance. There might be greater benefit from a variety of models linking certified qualifications and/or experience to a range of skills or competencies, including knowledge of relevant legal and regulatory matters, relevant law enforcement practices and appropriate working practices.

1.4 At the previous workshop on inputs to the Police Reform White Paper a senior private sector security professional, a serving police officer and Chris Sundt (sometime principle security consultant for ICL and main rapporteur for the EURIM-IPPR E-Crime Study) agreed to do papers on the issues they felt needed to be covered, from their differing perspectives. These are attached as appendices 1, 2 and 3 and indicate clearly some of the models that are most obviously worth exploring as well some of the issues that need to be addressed.

1.5 This meeting would explore the possibilities for different models.

2. Discussion

2.1 A first need is to ensure that current routines for making industry expertise to law enforcement become more effective and widespread. A meeting of the Strategic Stakeholders Group of the NHTCU on the previous day had raised the issue of industry liaison. The use of specialist staff from industry without commitment only works for so long. The need for commitment should be brought out in any discussion of the different types of liaison.

2.2 There are potential cross-overs between the various models. For example at least one major supplier wishes to explore the practicality of giving Computer Crime Units access to their high level technical support staff. What are the issues regarding vetting, liabilities etc. if 'specials' are not volunteers but corporate staff helping the police (whether ad hoc or a routine basis) as part of their mainstream professional duties? Would there be a requirement for such staff to be available to appear in court if they had given assistance?

2.3 Discussions are already under way on such co-operation and there are indeed many issues to be addressed. The way forward is not to jump at specific models but to test possible routines with pilots which, if successful, can be templated. Standard answers to frequently asked questions are central to industry technical support services and the production of such material for direct use by CCUs should be a core part of such pilots.

2.4 Among the other ideas which had been put forward recently were the creation of operational links between lead civilian law enforcement teams, those parts of Government with access to leading-edge filtering and track and trace technologies for National Security purposes and the security and abuse teams of the main Internet and Communications providers.

2.5 Thus a specialist child protection unit based on Cambridge might work with the Internet Watch Foundation and be able to draw on rings of part-time professionals, volunteers and both University and Corporate resource as well as that of different parts of Government. A specialist unit based in London might similarly draw on the expertise of UCL and its partners in both Government and Industry.

2.6 Such concepts raised many issues of organisation and governance but, if the issues really were as serious as was claimed, should these not be discussed rather than dismissed as impossible because they did not fit current models.

2.7 The counter-view was that this pattern would create more complexity and that we should begin with ideas which fitted with current methods of working and were comparatively easy to implement, rather than jeopardise practical progress by being over-ambitious

2.8 Vetting, training and payment are major issues but the shake-out during the high tech recession and the growth of off-shore outsourcing means that there are now large pools of under-employed ICT professionals potentially available as either volunteers or part-timers. ONS statistics indicate that over 125,000 ICT staff were made redundant last year. Industry statistics (CEL) show that thousands of women professionals leave each year to look after children or elderly relatives. Could their talents not be cost-effectively harnessed through retraining in, for example, computer forensics? There are also tens of thousands of computer science students seeking part-time employment. Several Universities (e.g. Greenwich) have routines to enable them to obtain proprietary certifications and part-time industry placements early in their courses so they can earn rather more than by stacking shelves in the local supermarket.

2.9 There are already a variety of models for employing part-timers with specific skills and those qualified in other professions, from interpreters to medical practitioners but 'true volunteers' like the Police Special Constables are unpaid. Remunerating those without specific skills or qualifications would create problems.

2.10 The specialist accountants being recruited to the Fraud Squad have the full powers of a warranted special constable. This enables them to be given access to otherwise confidential material and to accompany the named officers on a raid without having themselves to be named on the warrant. It also gives them credibility within the police service because they are formally trained (like all special constables) in police practices and procedures such as evidence gathering and presentation and are under police governance. They are, however, appointed as warranted 'special constables' for an indeterminate term of office, which means that they must be under 55 when appointed and be physically fit for normal police duties even though they are not expected to perform them.

2.11 This rules out the use of the disabled (a particular problem since ICT has long been viewed as one of those careers where physical disability should not be a bar to employability) and the 'silver surfers' - those over 55 who have moved into part-time employment. According to BT research, this group is likely to spend far more time on the Internet than those in the 35 - 55 age group and US experience appears to show that teaming retired ICT professional with retired law enforcement professionals under law enforcement governance can be a very effective means of identifying and reporting malpractice.

2.12 Special constables are normally vetted as for police recruits with references taken up and a Criminal Records Bureau check but there are no financial checks. Few police recruits or secondees from industry or other law enforcement agencies currently have security clearance unless working with units which routinely require this. The standard minimum commitment is 200 hours/annum or 4 hours/week and most do two 8 hours tours of duty per week, aggregated into batches. The hours of the accounting specials (only just being appointed) are expected to be more flexible and ICT specials might be expected to put in similarly flexible hours working on specific projects or supporting specific investigations, rather than putting in so many hours a week.

2.13 The TA model with retainer payments and pay while on duty does not exist in the UK police service. This raises possible problems with motivating specialists to be available for specific tasks - although recent changes to TA terms and conditions may have led to a similar situation and it is said that the current routines (as opposed to those which prevailed until recent changes) should not be viewed as a model. While some specialists might volunteer to go on a skills lists to be called on when needed, others would want a regular involvement. Experience in other areas with ad hoc registers of volunteer experts is patchy - they easily become out-of-date and inaccurate.

2.14 Other options also need to be considered - e.g. where individuals are 'encouraged' by their company to act as 'corporate specials' as part of their job. Their time might be charged to the corporate budget, but liability remained an issue. For warranted specials, liability lay with the police but what would be the position of a 'corporate special' coming across criminal activity in the course of his or her normal working day.

2.15 What is the position of railway company staff who are also Transport Police Specials? The answer was that the police were liable whenever specials placed themselves on duty. An initiative by the Metropolitan Police - Shopwatch - would be announced very shortly by which selected shops (e.g. Dixons) would permit staff members to volunteer as specials ½ a day per week, paid by the employer. Such specials would be deployed on the 'high street' or in the shopping centre where they normally worked. Volunteers would also be able to open currently closed police stations for taking reports and similar administrative duties. Community Support Officers, however, were paid.

2.16 Special constable status does not appear to provide any advantage to, for example, a member of an ISP abuse team wishing to report and initiate action under the Sexual Offences Act or a bank security employee wishing to initiate action on a phishing expedition or other fraud. Their status would be no different to that of any other professional. It cannot be used as a means of bringing security staff wishing to protect their organisation from attack under a police umbrella. It is more important to give basic training on how to respond to the problem, including how to report the incident and preserve the evidence.

2.17 Different sorts of people are required for different causes. Deep technical support would be freely offered by most suppliers for current investigations if the need was both genuine and urgent but computer forensic skills were in short supply and would not be offered for free by corporations, unless it was in their interests. However, there are also a growing number of retired specialists and those with in-depth technical skills no longer in demand who could be cross-trained. We need both to connect professional specialists to those who wanted their services and would pay, and also routines for volunteers of all ages who had, or could acquire, the necessary expertise and experience at reasonable cost (to whom?).

2.18 Whether we were talking of permanent and regular relationships (e.g. special constables attached to specific computer crime units) or intermittent relationships (e.g. national experts in specific areas) we needed to consider how they would be brought into 'the police family' since motivation commonly requires physical, geographic contact as part of a team as well as regular practice. There is also the issue of handling the career progressions of currently employed professionals since the current 'one-size-fits-all' framework has no provisions for terminating the status of a 'special constable' unless they themselves resign or for ring-fencing the duties or term for which they are warranted.

2.19 There was discussion as to whether the Community Support Officers programme might provide a model - current CSO's are permanently employed and though not warranted, are the 'eyes and ears' of the police, able to act as professional witnesses. Given the problem of unreported and therefore unaddressed computer crime, could we use 'chat-room' volunteer CSOs from the ranks of senior citizens, mothers and the disabled, under police supervision, working from home or authorised premises as in some US programmes? The skills level needed is well above that for CSOs and those involved would need training and authorisation under RIPA.

3 Conclusions

3.1 A number of the models used in other countries do not fit with the current UK policing environment.

3.2 Current UK frameworks allowed for the employment of the disabled and over 55s as part-time professionals but not as volunteers. Therefore while we should be able to make a number of 'quick win' recommendations within existing legal frameworks, there is also a need to look at some of the constraints.

3.3 Given the complexity of the situation and the potential controversy of some of the options that we might flag for examination, we should drop plans for early publicity for recommendations in this area.

3.4 Instead PV would draft the EURIM response for the Police Reform White Paper (target being for review on 22nd January) and Chris Sundt would redraft his paper on Access to Specialist Skills (revised version attached as Appendix 3).

Appendix 1 The case for Specialist Constables: from the perspective of a senior private sector line security professional with operational responsibility

Given the explosive growth in high technology crime as is evidenced in the annual CSI/FBI (<http://www.gocsi.com/awareness/fbi.jhtml>) and the annual DTI Information Security Breaches Survey (http://www.dti.gov.uk/industries/information_security/downloads.html), there has not been a comparable expansion in the personnel, resources and skills need to counter this ever expanding issue. This is coupled with a significant lead-time to develop the appropriate investigative and technical skills required. Many cases require a high level of specialist expertise that would not necessarily be easily found within law enforcement. In a significant number of cases an outside expert may be required to properly investigate the case. This brings in the issue of proper vetting.

Properly trained specialist constables could help to relieve this burden from law enforcement. I believe this program is a win-win-win for law enforcement, the community and industry. Such a program would allow the Home Office and local constabularies the ability to place specialist constables in roles where their unique talents can be more effectively utilized by the community. This program would give law enforcement and thus the community, access to skills they might not otherwise be able to access or be able to easily afford.

It is not envisioned that these specialist constables take an active part in field operations, but more of a technical advisory role. However, there may be instances in which a specialist constable is required in the field or on a more sensitive case. My recommendation would be a two tier system for specialist constables:

- Tier One (Technical Advisory role):
 - Counter Terrorist vetted (CT)
 - No field activity to be undertaken
 - No prior military, law enforcement or intelligence background required.
 - Little or no law enforcement training required
- Tier Two (Technical Advisory role and Field Operations)
 - Security Cleared (SC) or better
 - Field Operations allowed
 - Prior military, law enforcement or intelligence background required
 - Standard Special Constable training required

The candidates would be recruited and trained by their local constabularies to a nationally agreed upon standard. However, a centralised skills and language database would be held by the Home Office, the National High Tech Crime Unit (NHTCU), the Crime Faculty based at Centrex or similar location. This database would be accessible by all local law enforcement.

Individuals with a generalist skills set will tend to be utilized with more frequency than individuals with a narrowly defined skills set. Given enough recruits, there may be instances where the generalist may not have enough work to maintain interests. Therefore the specialist constables should be engaged in not only a technical advisory role, but on projects as well. Some examples could include intelligence gathering, vulnerability research, developing investigative techniques for current and emerging technology and developing training programs, to name a few.

In conclusion, I believe this program is needed by UK law enforcement to get them appropriate access to the skills they require, to forge closer ties with industry and the community which will assist them in combating this ever increasing issue. It's good for the community, it's good government and it's good for law enforcement.

Appendix 2 Why we need Specials: from the perspective of a police officer

Essentially Hi-Tech crime has grown from nothing to the current level in about 20 years - with no commensurate increase in police resources. In addition, the technical knowledge required to progress Hi Tech crime investigations requires a significant lead time for detectives to acquire.

It is often the case that an investigation requires such a high level of competence with a particular type of software or hardware that a dedicated specialist in that area must be brought in for a one-off assignment. This can cause problems as this individual may not be vetted and indeed may often work for a rival firm to that of the alleged victim or suspect.

These problems could be alleviated with prior preparation and training of the people we are likely to ask for assistance:

- Vetting to SC level (cost implications)
- Basic training on evidential handling and legal aspects of their work
- Sign-up to Official Secrets Act

This basic preparation would clearly provide police with a pool of specialists who are cleared and trained to assist with particular tasks on a one off basis.

Two key aspects must be understood:

- It is not envisaged that these 'specials' would be used operationally on searches so there are limited safety implications. They would not necessarily carry a warrant card and would not therefore need physical training.
- There is no requirement for regionalisation as, once the checks have been done, most of the interaction will usually be via email and phone call - they would rarely need to meet in person. Indeed, there is no reason the 'special' needs to even be resident in the UK.

The organisation of this cadre of specials is significantly different to the current specials arrangement and also from that of the TA (often cited as an alternative model). The list of vetted and trained individuals should be managed centrally (probably by the NHTCU or the Home Office Hi-Tech Crime unit) - with local CCU's calling up for a name for a particular specialism such as 'hacks of CheckPoint firewall software'.

There is a strategic decision regarding the tasking of these specials - will they only be used for one off jobs where their particular skills are required or will they be tasked with more general and generic types of investigations? One off investigations will possibly not occur with sufficient frequency to keep their interest but more generic tasking may incur further issues:

For example, tasking to research paedophile sites would almost certainly require expensive psychiatric vetting and may attract specials with nefarious motives. Tasking to research specific hackers on IRC would require a level of legal training and supervision that may make the task financially unviable.

The use of 'specials' to tackle volume crime (such as auction fraud) is an attractive prospect but may not use their skills to a sufficient extent to maintain individual interest. There is also the argument that UK policing ought to be supplying detectives for this relatively unskilled task - we are looking to use specials with high end skills that our detectives simply do not possess.

There is a great deal of work to do before we are ready to start the recruitment and vetting process. It is clear from anecdotal evidence that there is a large pool of potential specials and also a need for a more statutory footing on which to base the current casual use of individuals by police.

Appendix 3 Law Enforcement access to Specialist Skills: paper by Chris Sundt

The EURIM-IPPR paper on Roles and Procedures for Investigation suggests that law enforcement could make greater use of specialist expertise from industry. The Consultation paper on *Policing: Building Safer Communities Together* makes, in paragraph 4.21, much the same suggestion. This note reflects discussion at EURIM workshops on this area that raised a number of practical issues associated with the greater use of specialist expertise.

This paper is in two parts. Part 1 discusses issues around the availability of specialist skills and expertise to law enforcement. Part 2 proposes specific processes and responsibilities to stimulate debate.

Discussion at the EURIM workshops identified an initial range of skills that might provide immediate advantage. They include:

- Those with expertise to assist in the investigation of crimes that include a computer and/or network-related element. Such expertise may range from incidental advice on the interpretation of specific technical evidence carried out off-line to direct assistance in the investigation of complex technical situations in real time. Effort involved may vary from the odd few hours spread over a period of time to an intensive few days of concentrated effort.
- Presentation of evidence in court in support of the prosecution case – however this is comparatively rare at the moment.
- Advice on how specific technologies work, or how they are exploited commercially and might be used. Such information can be used to assist in development of approaches to the investigation of crime.

However this paper makes no assumptions about the range of competencies and skills that might be made use of by law enforcement. It considers the broader issues associated with the greater use of expertise in the private sector by law enforcement.

Part 1 – What is involved

Given the explosive growth in high technology crime as is evidenced in the annual CSI/FBI (<http://www.gocsi.com/awareness/fbi.jhtml>) and the annual DTI Information Security Breaches Survey (http://www.dti.gov.uk/industries/information_security/downloads.html), there has not been a comparable expansion in the personnel, resources and skills law enforcement need to counter this ever expanding issue. This is coupled with a significant lead time to develop the appropriate investigative and technical skills required. Many cases require a high level of specialist expertise that would not necessarily be easily found within law enforcement. It is often the case that an investigation requires such a high level of competence with a particular type of software or hardware that a dedicated specialist in that area must be brought in for a one-off assignment. This can cause problems as this individual may not be vetted and indeed may often work for a rival firm to that of the alleged victim or suspect. Properly trained specialist resources could help to relieve this burden from law enforcement. Such a program would allow the Home Office and local constabularies the ability to place specialists in roles where their unique talents can be more effectively utilised by the community. Such a programme would give law enforcement and thus the community, access to skills they might not otherwise be able to access or be able to easily afford.

If there is to be true partnership between law enforcement and the private sector, this must be based on properly formed arrangements and not rely on the goodwill of industry. As such resource becomes a more integral part of the overall law enforcement activity, matters such as liability, confidentiality, motivation and the legal framework within which such people work become significant and must be addressed.

There are three aspects to industry liaison/partnership that need to be considered. Any scheme must be clear about which combinations of these areas it does, and does not, address. Note that this discussion excludes support provided through normal commercial arrangements such as consultancy contracts or managed service contracts, for example. The three types are:

- Types of access

- Types of person
- Relationship with law enforcement.

Types of Access

- Access to deep support, to product support and to expertise on specific technologies. This can only be provided by the suppliers of those systems or technologies. As currently, it is almost always provided on a pro bono basis. However, there may be advantage in formalising these arrangements in certain cases, as discussed later.
- Access to persons with specific expertise and/or skills of use to law enforcement in particular situations or in support of particular teams or operations.

Types of Person

- Volunteers who offer their services as individuals free of charge. Note that there is a marked trend away from volunteering for a variety of reasons, not least the increasing need for volunteers to undergo various checks⁷.
- Employees whose time is made available by their employer without charge.
- Individuals who offer their services, or employees whose services are made available, on some formalised contractual basis which may include financial or other forms of consideration.
- Individuals made available on some formalised seconded/loan or other basis by their employees.

Persons may be made available at employee discretion, as an individual on call or available to an agreed schedule, or as part of a joint team (either full-time or part-time). Persons with the necessary skills and experience can be drawn from a broad church. Those actively working with these skills may have only limited free time available to devote to support of law enforcement because of work and/or personal commitments. There is a pool of experienced people who are no longer in fulltime employment with the potential to offer significant time to such support. However, there may be issues relating to how they maintain their knowledge and experience over time. There are other potential pools of expertise that might offer specific skills such as graduate students and those who can only work from home. Indeed, in many cases communication may be by email or phone call and there may be no need for the individual to be physically part of a law enforcement team or even resident in the UK. Any scheme should allow people from all potential communities to participate.

Relationship with Law Enforcement

Any person providing specialist services to law enforcement can operate with one or more of the following attributes:

- As an individual with no particular law enforcement-related attributes.
- Subject only to CRB checks and verification of references.
- Sent through basic police training appropriate for their role.
- Warranted (which is equivalent to becoming a Special Constable).
- Subject to the Official Secrets Act.
- Security cleared.

Discussion

This analysis makes clear that there are many different scenarios for the use of specialist expertise and skills by law enforcement. In part this is because of the diverse range of activities that such persons could become involved in.

People responding to requests for deep product support may just be employees in a supplier responding to queries. For major suppliers there may be advantage in a formal process being created whereby such requests are channelled through a central PoC that collates and records all such requests, building up a FAQ database to reduce the load on the support staff.

⁷ For example see The Economist for 10 January 2004 page 21.

It may even be useful for one or two key staff to be cleared and/or trained in police techniques to enable them to interact more effectively with law enforcement.

People in joint teams, such as the existing DCPCU, may best be fully warranted.

People providing specific expertise, skills or knowledge should be cleared and trained to the level appropriate to the tasks for which they are most likely to be used by law enforcement. It is not envisioned or required that such specialists take an active part in operations in the field, but play more of a technical advisory role. However, there may be instances in which a specialist is required in the field or on a more sensitive case. A two tier system for specialists could be considered. The normal technical advisory role could require only a basic CRB check with only basic enforcement training. Field activity would rarely, if ever, be undertaken. Those involved in particularly sensitive technical advisory roles or expected to be involved in field operations may need to be security cleared (SC) or better and undergo at least training equivalent to that undergone by current Special Constables. Prior military, law enforcement or intelligence background would also be an advantage in such cases.

Whether those providing specific expertise on an ad-hoc basis need to be warranted is open to debate. It may well be a benefit for those whose services are regularly called upon. However, the current Special Constable scheme may not be a suitable vehicle for warranting ad-hoc provision of services. In particular there is a maximum age at which a Special Constable can be appointed (55) which would rule out those retired, for example, offering their services, and a Special Constable must be physically fit and able to carry out the office of constable, which would rule out those house-bound, disabled and the like.

There is a strategic decision regarding the tasking of these specialists - will they only be used for one off jobs where their particular skills are required or will they be tasked with more general and generic types of investigations? One off investigations will possibly not occur with sufficient frequency to keep their interest but more generic tasking may incur further issues. For example, tasking to research paedophile sites would almost certainly require expensive psychiatric vetting and may attract specials with nefarious motives. Tasking to research specific hackers on IRC would require a level of legal training and supervision that may make the task financially unviable.

The use of specialists to tackle volume crime (such as auction fraud) is an attractive prospect but may not use their skills to a sufficient extent to maintain individual interest. There is also the argument that UK policing ought to be supplying detectives for this relatively unskilled task – law enforcement is looking to use specials with high end skills that their detectives simply do not possess.

Legal Implications

Initial analysis suggests that the current legal frameworks for Special Constables, Community Support Officers and the like will not provide an adequate framework for the retention of all types of persons who should be encouraged to offer their services in support of law enforcement. In particular there may be a need to include legal processes for warranted persons who cannot become Constables for physical or personal reasons. It may be necessary to create new legal entities that enable such persons to be appropriately remunerated and retained under some formal law enforcement relationship that allows them to operate effectively with law enforcement teams without themselves being fully warranted.

Part 2 – Processes and Procedures

To stimulate discussion, a scheme for the registration of people who can provide specialist services to law enforcement is described below. This scheme includes for some issues the sorts of questions that need addressing for any such scheme to be implemented. To minimise complexity, the scheme includes within a single process the ability to handle people with a wide spread of skills and availability, and different relationships with law enforcement.

It is proposed that a central Register of individuals with specialist expertise be established (possibly within the NHTCU and accessible via the secure Intranet). Individuals would be sponsored for inclusion on the Register by local police forces on the basis of personal

knowledge. However, there would be a formal process to validate the competence and skills of candidates, and to verify their personal suitability as a candidate. All persons on the Register would be required to undertake training appropriate to the roles and responsibilities they will undertake when working in support of law enforcement, and would be expected to maintain their competence over time. Law enforcement officers requiring particular expertise would identify suitable persons on the Register. Their suitability can be verified in discussion with their sponsor (who would maintain contact with all those they sponsor) before a request is made for their assistance.

Associated with the Register would be governance rules, including statements of the responsibilities of the various parties, matters of confidentiality and liability and the commercial arrangements for compensating specialists for their time.

Purpose

- To establish a Register of individuals with specialist skills who can be called upon to support law enforcement.
- To describe the processes associated with that Register, and the governance rules that apply to those involved with it.

The Register

There will be a central Register of all individuals accepted as specialists and available to support law enforcement on request. The Register will contain at least:

- Personal details
- Accredited and/or verified competencies and skills – both technical and law enforcement related (for example, whether or not the person can act as a witness)
- Status in law enforcement terms (e.g., warranted, able to support field operations)
- Security status.
- Sponsoring local police force and contact details
- Availability profile including, for example, constraints on availability or location
- Remuneration arrangements
- A short list of previous occasions when this individual has supported law enforcement, with key activities carried out.
- Employer (where relevant)

The competencies and skills will need to be defined in a common form, and include any recognised qualifications.

The Registration Process

An individual will be sponsored for inclusion in the Register by a local police force on the basis of local knowledge and/or experience. A formal process will need to be agreed for vetting candidates as suitable. This will cover at least verification of the claimed skills and competencies of the individual, and a check against personal history. Where an individual is liable to be exposed directly to the criminal justice system (for example, as part of a team collecting evidence or appearance in the witness box) or to play an active part in field operations additional checks may need to be made to confirm suitability.

It is proposed that all approved individuals, before being placed on the Register, undergo training on aspects of the criminal justice system relevant to the role(s) they might play in support of law enforcement – especially matters such as investigation techniques, preservation of evidence and constraints on what action can be taken. It may be desirable for all individuals to undergo refresher training from time to time depending on the rate of change of relevant legislation and guidance and the extent to which an individual has been involved in supporting law enforcement.

There may be a case for some individuals to be at least SC cleared – but this will depend on likely use and cost implications.

The sponsor will remain responsible for verifying that a sponsored individual retains their competencies and skills, and their availability.

The Approval Process

Currently there are very few qualifications that would automatically confirm the competencies and skills claimed by an individual. It is likely that a peer review process, such as that used by the BCS for the Security Practitioner's Register would offer the best approach initially. There are organisations, such as ICAF and CRFP, that might be considered competent to confirm the competencies of individuals in specific disciplines through agreed processes. Personal history is best addressed through the CRB and through direct local knowledge – although any requirement to undergo an SC vet might replace this.

Accessing Specialist Expertise

All local police forces will have direct access to the Register. Access would be available to all branches involved in investigations, not just to Computer Crime Units – since there will be many situations where a computer system is involved, but is not the prime target of the investigation. In many cases a local force will have access to known local specialist expertise and will not need to use the Register. Where additional expertise is required, potential candidates will be identified by a search of the Register. The suitability of selected candidates for the task in hand can be verified with the sponsor, who should have first-hand knowledge of the individual. Whether the candidate is approached by the sponsor or the requesting force is up to those involved.

Identifying Specialists

Many specialists will be known to local police forces, and recommended by them after discussion with the individual concerned. Individuals may offer themselves for consideration, or organisations may choose to offer employees for consideration. There are classes of individual whose expertise may be readily available – such as retired people and those with disabilities that restrict their mobility – who could be encouraged to volunteer. How this might best be achieved would need thought.

Once a specialist has been identified, and indicated willingness to be included in the Register, suitability needs to be verified. The commitment by, and responsibilities on the individual need to be made clear, and any constraints on availability established. This is of particular importance where the individual is in employment as they would be included on the Register as an individual, but the employer needs to understand and accept the employee's position. Normally an employee would be expected to be available to law enforcement outside normal working hours, but there will be occasions where greater commitment is advantageous – in this case, the employer may decide to accept (or even support) the absence of the individual, or expect recompense for their absence. The principle should be that neither the individual nor the employer is disadvantaged.

Role of Sponsor

The sponsor would normally be a local police force. They would be the point of contact for volunteers as candidate specialists – who would tend to be from the area covered by that force.

The sponsor would initiate all necessary checks – using whatever verification processes are established. They would also be responsible for arranging for candidate specialists to attend any necessary courses.

The sponsor should arrange gatherings of specialists for whom they are responsible to create a sense of belonging, to keep them up to date on any legal or procedural issues that might affect them, to provide a forum within which they can exchange experiences and ideas, and to ensure that they are maintaining their expertise and legal knowledge. Such gatherings might include all specialists in the area and/or bring together just those with particular skills.

The sponsor will also provide a point of contact through which other forces can obtain background information on the suitability of specialists for which that force is responsible.

Governance Issues

There are a number of governance issues that need to be resolved. Key ones are noted here as a basis for discussion.

Contractual Arrangements

A standard form of contract should be developed that covers the terms and conditions under which an individual offers their services. Since individuals will be “called up” it should take the form of a tasking contract – defining detail such as the minimum notice for call-up, any constraints on the availability of the individual, and similar information relating to the use of that individual. While all individuals would be encouraged to accept the standard terms, there will be individuals who require changes for personal or professional reasons.

Confidentiality

Since anyone working in support of law enforcement may become aware of sensitive information the contract should include confidentiality statements even if there is a requirement for them to sign the Official Secrets Act – as this does not necessarily cover confidentiality of personal data or commercially sensitive data.

Liability

Where liability rests needs to be made clear for all types of relationship between the person and law enforcement. While this may be documented where the person is warranted and is acting in that capacity, where the person is not warranted, or is working under some other formal arrangement, liability needs to be defined. The liability issue is of particular importance in the grey area where the person may be acting outside a formal law enforcement team – for example, as part of an in-house investigation.

Remuneration

The contract should include any remuneration due. There are, potentially, three elements to any remuneration:

- A retainer paid for volunteering to be on the Register
- A fee covering time spent in support of law enforcement (for example, an hourly or daily rate)
- Agreement to reimburse expenses incurred while in support of law enforcement against an agreed scale of expenses.

As a minimum expenses should be paid on a reasonable basis (for example, actuals plus allowances for overnight stays, no-bill meals, etc). Whether a retainer should be paid is doubtful – but might encourage people to volunteer. Fees for time spent may be appropriate for some types of specialist support, but the amount needs to be agreed. The market rate for independent consultants (which is significantly less than that paid to employees of consultancy companies) might be a good target. Whether an individual accepts payment, and at what level, for time spent supporting law enforcement will depend on their personal circumstances, on the type of support offered and, if an employee, the policies of their employer.

Commercial Sensitivities

An issue that needs to be addressed is that of commercial confidentiality. While contractual confidentiality clauses can bind people to respecting confidentiality, there could be cases where an individual employed by one company could be supporting an investigation that involved, in some way, a competing company – for example an employee of ISP A is asked to support an investigation that involves criminal activity that exploits the services of ISP B. This could create commercial tensions where the specialist could gain commercially sensitive information on the business of the other company. This is best covered by a process that requires investigators to be aware of potential conflicts of interest, and to ensure informally that both parties are happy with the use of the selected specialist.

Working Methods

Specialists on the register should have undergone at least basic training on law enforcement methods – for example basic investigation techniques. However, there will be particular methods and operating rules appropriate to specific activities (such as investigations) and teams for which additional training may be appropriate. These should be written down and agreed with the specialist before involvement in a specific activity. Indeed, the ability to operate according to specific rules may be a factor in selecting appropriate specialists.

Deliverables

The contract is unlikely to define in any sensible form the deliverables as these will vary from task to task. However, a specialist needs a clear definition of what is expected of him, and in what timescale, as part of their assignment in support of law enforcement. This should be available as part of the criteria for selection of suitable specialists by a law enforcement team.

Law Enforcement Implications

Note: This is a holding space. I think there is a lot that needs to be said here.

There needs to be clear statements as to what place specialists on the Register have in the law enforcement structure.

Are they:

- Private citizens on call to specific law enforcement teams as consultants on request.
- Empowered as, for example, some form of “special constable” with identified legal powers to assist them in their work in support of law enforcement.
- Part of an ancillary law enforcement structure such as that for Community Support Officers, but with a remit relating specifically to the technical support role of specialists.
- Fully warranted with all that entails.

Or are they included in some other way. How they fit in may well also affect how they are remunerated, and from whose funds any payments come.