



**Report of the EURIM E-Crime review of progress, held on
13 April 2005 in Room 134, 1030-1230, 2 Millbank, Westminster**

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

1. Introduction

1.1 Philip Virgo as Chair opened the meeting and invited introductions, commenting that all discussion would be off the record but that a summary report, without attributing participants, would be produced for circulation.

2. Current state of play on Home Office consultations

2.1 There appear to be 4 current issues:

- Police Reform consultation
- Child Protection on the Internet consultation
- E-Crime Strategy consultation
- Reporting issues

Police reform

2.2 The consultation period ended on 8 October 2004, and the Government published its White Paper on Police Reform 'Building Communities, Beating Crime: A better police service for the 21st century' in November 2004. The consultation period for the White Paper finished at the end of February 2005. A number of responses on e-crime were received, including from CBI, IoD and EURIM.

2.3 Responses were generally broadly positive and supportive of measures such as greater accountability and working with communities and businesses. Some concerns were expressed about structures and resources. Issues raised by CBI, IoD and EURIM referred to IT crime not being geographic and therefore a specialist area. There was some debate about the impact of computer forensics on investigations, and whether e-crime is a specialist area or should become an integral part of police investigations

2.4 Although the last Government made no firm decisions before the dissolution of Parliament, it is clear that policing and policing structures are politically important, and will be high on the agenda of any new Government. The responses to the White Paper will guide decision-making.

Child protection on the Internet

2.5 The last Government announced on 1 April 2005 the creation of a new national 'Centre for Child Protection on the Internet'. Much of the operational remit has yet to be decided, but it will focus exclusively on child protection rather than Internet safety in general. It is envisaged that the Centre will also provide a 24/7 single point of contact for the public, law enforcers, industry and other organisations, for reporting the targeting of children online in England and Wales. The last Government intended the centre to be multi-agency, involving child protection professionals, industry support and offender management. The Centre will undertake crime prevention and crime reduction strategies to reduce the harm caused by online child abuse and launch proactive investigations to identify high priority targets.

2.6 All industry partners in the consultation exercise, including mobile and fixed Internet providers welcomed the idea of a SPOC, which should also provide an important resource for local as well as international police forces and organisations. The incoming Government (whichever party wins) will probably wish to advance the Centre rapidly, alongside the Serious Organised Crime Agency (SOCA), expected to be operational by April 2006.

2.7 On wider European issues, Insafe (<http://www.saferinternet.org/ww/en/pub/insafe/safety.htm>) provides internet safety-related information and serves as a coordination point for relevant activities in 16 countries. Childnet International have redesigned and relaunched their successful Chatdanger website following extensive research with children and young people. The website uses real life stories to demonstrate the potential dangers on interactive services and to give advice to children and young people about how to stay safe on chat, instant messaging, online games, email and mobile phones. Insafe funds projects in member states and across Europe for hotlines for reporting illegal content, public awareness campaigns for filtering and labelling etc. The Virtual Global Task Force has been piloting online reporting, and it is possible to report to UK police online now. The pilot scheme shows that this is manageable, with positive results. The UK component of the VGTF will form part of the Centre.

2.8 The last Government made clear that the Centre for Child Protection on the Internet would not replace the IWF, although the exact Terms of Reference of the Centre are yet to be determined by the new administration.

2.9 Primary responsibility for child protection and dealing with individual offenders will remain with the local police force, but it is hoped that the Centre for Child Protection on the Internet will provide proactive prevention and deterrence to reduce the incidence of casual access to child pornography. Local policing effort will be expected to focus on high priority targets identified by the Centre, rather than those sent by international law enforcement bodies. The Centre will also act as a 'centre of excellence' and support resource for local forces.

2.10 The last Government envisaged a strong role for the Centre in developing skills and sharing expertise, but training needs would probably continue to be delivered through existing agencies, e.g. Centrex (Central Police Training and Development Authority) for specialist police training (which the Centre may support), and the universities for social services training.

2.11 The Centre would be alert to how children and paedophiles are using chat rooms, and how they might (ab)use new positioning technologies such as the delivery of highly personalized, location-based services, predicted to take off in late 2005 to early 2006 (<http://www.lbszone.com/content/view/19/2/>).

National E-crime Strategy

2.12 The last Government announced few details of the strategy, but ministers, officials and external stakeholders amassed a considerable body of work, with recommendations, that will be available to new ministers if and when they decide to publish an e-crime strategy.

2.13 **Police structures are likely to be a major plank of any national strategy, and computer-related crime would be an essential part of the police reform agenda.** Internet content and websites, skills, e-crime reduction, including the work of Project Endurance, are all likely to feature strongly in the new agenda.

2.14 The work that EURIM was doing on skills was a useful reference, and there was a need now to focus on action rather than spreading the agenda more widely. California law now requires firms to disclose unauthorised access incidents to the client base when they are discovered, but although talks had been held on this, there are no active plans to implement this in other states to deter identity theft - there are no known cases of prosecutions under California law. However, if people thought this was a good idea, now would be a good time to put it on the table.

2.15 There has not been a great deal of discussion on issues of content where this involves publishing cheaply and easily through electronic media, and **ministers may well decide to follow up on this, e.g. BT filtering of child abuse websites.** However, there is unlikely to be consultation on the use of reasonable force in self-defence (e.g. hacking back), where the legal position was felt to be reasonably clear. Issues around convergence e.g. fixed internet content and mobile phones are very

dynamic, and may require more debate. Botnets (compromised computers) and 'commercial' hacking have become serious issues. Another industry issue is ownership of liability in cases of filtering where inappropriate content is allowed through.

2.16 Consensual demand is high for amendment of the Computer Misuse Act, and to prevent further delay there is a need to provide relevant material to the new intake of MPs in order to produce a climate for early implementation in the legislative programme.

2.17 End-to-end IP networks have enhanced the possibility of attack and the infrastructure itself is now highly vulnerable, with serious implications for critical national infrastructure. These are being addressed. There are a variety of services on the IP network, e.g. VoIP, VIDEOoIP, that are subject to criminal tampering. Built-in product security should be standard practice. It is important however to act proactively to get people to take responsibility for their own behaviour, and not try to rely on regulating against all eventualities – which would be impossible. This might start with good citizenship lessons in primary school, including advice on protecting children not just from predatory adults, but from each other (cyberbullying etc.).

2.18 The Foresight Cyber Trust and Crime Prevention project uses science and imaginative future scenarios to highlight the challenges facing policy makers, businesses and the public by the rapid development of ICT if there is to be future trust in the Internet. This group needs to be aware of the project's work in enabling technology to be used to reduce existing crime, and to reduce the extent to which technology extends the scope of existing crimes, or introduces new forms of crime. Should this be within the remit of Skills for Justice?

2.19 Skills for Justice' remit is to ensure provision of adequate training and skills strategies; this would be appropriate in the field of e-crime, but not for a wider scope. Home Office, DTI and DfES should be brought together to rationalise a number of disjointed activities that were currently creating different skills sets. Educational materials for the new intake of MPs should cover the question of "which minister(s) should lead (and co-ordinate the others) on which issues?" The current joint study by e-skills and Skills for Justice is pulling together the skills definitions and frameworks, but is not addressing the development and delivery of training. If implementation policy is the responsibility of DfES, then we would want a DfES minister to lead as part of a tripartite DfES-DTI-Home Office exercise. The National E-crime Strategy, as a Home Office document, can be expected to include linking statements to the work of others but there is also a need for clarity as to who will be delivering the linked programmes.

2.20 Schools were still not part of the Skills for Justice strategy; DfES involvement is needed, with information systems built early into schools programmes. We need to contact those working regularly with DfES to help close this loop, but progress will probably depend on securing a coordinator within the ministerial team. An overarching strategy can founder if Government departments continue to work in silos with no individual or department taking ownership for components. Although Government papers may bind all affected departments, resources are more likely to be committed if ownership is allocated. It may be useful to produce a paper identifying the issues and players, with recommendations based on the assumption that this will be a DfES exercise. Schools sometimes have no dedicated IT staff - should minimum standards be in place in schools and public sector organisations for reducing crime? (The need for action by public sector organisations will be covered in the workshop on 4th May on reducing vulnerabilities).

2.21 Education is an essential part of security. A major issue is to ensure that teachers have the necessary materials and training. Cisco Systems staff present to schools on a voluntary basis, but it would be useful for security to be part of the school curriculum – Cisco provides networking qualifications in their academy. Informal talks here might help identify current initiatives and identify where more support is needed and potentially available. Project Endurance is not targeted or resourced to address schools. Victoria Petrucci has been appointed as programme manager to pull the threads together, focusing on ensuring awareness and action on the part of consumers and SMEs.

2.22 Listing the many initiatives on Internet security on a website would provide a useful information source, **and IEE agreed in principle to host and maintain free of charge a list of activities and initiatives as URLs.** Organisations wishing to have more exposure should send details to Graham Paterson (GPaterson@iee.org.uk). **A planning meeting will be organised for interested parties.**

2.23 The cost of regulation, compliance, fraud and e-crime is an increasing burden for UK industry which attracts little support from Government, while compliance with the US Sarbanes-Oxley Act has been said to cost as much as 2% of turnover. Trust in online transactions was higher with banks than with ISPs, because the banks accepted the risk – but how long can this continue? How soon would trust collapse if banks transferred the risk? There are a number of recommendations on data retention (not just those referring only to communications data as required under RIPA) and storage that have been accepted but not put in place. What is the balance of cost and risk? What should users (both public and private) as well as suppliers be doing? The debate also involves content data and storage, and therefore DTI (and application/content regulators such as FSA) and others, as well as Home Office. There are also liability issues. Clarification is needed on data preservation (including maintenance and security) as well as retention. Guidance is needed on whether (and how) to transfer bulk data to new media because formats (and thus accessibility) are subject to continual change.

2.24 The E-Business Regulatory Alliance is developing an 'e-radar' to identify and link to the top e-business legal issues of concern to organisations. Liability issues connected with content and spam are a major concern to ERA's largest members (BT and Amazon), and exercises are planned in this area (including a meeting with Nigel Hickson of DTI on 13 May, and a DTI workshop on spam). Details will be circulated.

2.25 Responsibility for International cooperation on law enforcement is shared between Home Office, FCO and the law enforcement agencies. Co-operation with most countries was said to be good at all levels. The issues of practical co-operation had had much attention over recent months and it was felt that political activity in this area was currently unnecessary and could be counter-productive, apart from the need to work with others (such as ISPA/APIG) to secure action on penalties under the CMA.

2.26 Amending the Computer Misuse Act to create offences in connection with denial of service and section 1 offences would be welcomed by industry and other stakeholders. Derek Wyatt MP, Chair of APIG, moved a 10 Minute Rule Motion on 5 April, emphasising that it is essential for a law to be in place to make prosecution possible when offences are committed, because that will send a strong and unambiguous message that e-crime is treated with the utmost seriousness. International co-operation is also key: increasing sentences for section 1 offences to two years will create an extraditable offence, and bring the law into line with the European cybercrime convention.

2.27 Skills for Justice personnel are involved in a number of projects tackling e-crime, and are collating information on work that has already been done on developing skills and competencies. S4J is also keen to attract stakeholders who would like to be involved in the current consultation on e-skills and competencies, and would particularly like input on mobile security. Vodafone offered to supply a contact for this. A prime concern is to specify the security skills that staff need, e.g. in police forensic capability, and to attract people to work with S4J to identify and develop skills.

2.28 Access to databases needs to be secure from both external (hacking) and *internal* (personnel) attack. With typical staff turnover of 20% p.a., vetting is problematical. Inevitably, some untrustworthy staff will gain trusted positions with access to databases, such as bank account details. Keyloggers have been generally found to be installed by internal employees. Central Government databases are natural targets for criminals. This is being addressed on 4th May.

3. Summary actions

3.1 Actions agreed include:

- a workshop to produce a paper on the provision of adequate training and skills strategies, and which departments should lead on what issues (discuss with S4J steering group);
- a workshop to produce a paper on good citizenship and security awareness programmes in schools (Cisco to host and chair);
- collaboration between CBI, ERA and TIF on data retention: including Govt/Regulatory issues;
- ensure reporting issues are highlighted in the briefing material for the new intake of MPs;
- ensure that the need for urgency in amending the CMA is a key message in the briefing material for the new intake of MPs;
- IEE to host and maintain a list of activities and initiatives on security in schools as URLs on its website;

- ERA to provide details of the DTI working party on spam, and liability issues connected with content and spam;
- EURIM to circulate information from POST on its future work on e-crime and security.
- EURIM to look at possible activity on Internet Content and on Liability issues, in co-operation APIG/ISPA and other relevant groups and to make a point of including representatives from the Mobile Sector because of the expected take-off in mobile broadband

4. Forward work programme

4.1 4th May: workshop to review paper on Reducing On-Line Vulnerabilities, including recommendations for action (both public and private sector) and possible guidance akin to that for SMEs now on the NHTCU.

4.2 Existing papers to be edited into briefing material for the new intake of MPs to help ensure political support and priority for action to implement already agreed recommendations.

4.3 Workshops to be organised as above to produce additional material.