



**Draft report of the E-Crime Group meeting, 16 September 2005, 0930-1230 hours  
at the Staples Room, Institute of Directors, 120 Pall Mall, London**

**Purpose:** to identify who is willing to work with whom to help pilot solutions to policing problems.

Chairman: Philip Virgo (EURIM); Rapporteur: Dave Wright (EURIM)

***SUMMARY OF MAIN POINTS***

1. Law enforcement lacks resources and has different priorities to industry. All police forces are overloaded, with none having the capacity to handle new business and engage in proactive policing with respect to computer related crime. Crimes against business, however serious, will rarely be investigated unless they fit local policing priorities. The City of London Police is the only force where those priorities include fraud and economic damage to the UK. The quality of the initial evidence as to the scale and nature of fraud and/or other economic damage and the availability of forensics of evidential quality will help determine what co-operation is offered.

2. The needs of the police for resources are many and varied, as are the resources available from industry. Industry needs structured requests to which it can respond, but most forces lack the skills to know what to ask for, let alone who to ask or how to make effective use of what may be available. Industry cannot be expected to organize studies of what law enforcement might need or how requests might be routed or structured.

**3. The agreed actions can be summarized as:**

- **help organize pilots on crime prevention in the Thames Valley and West Midlands areas building on what is already happening with a specific objective of establishing where skills from industry are available and can be used;**
- **EURIM to focus on changing the political climate so that law enforcement is better resourced and able to ask industry for the assistance it needs;**
- **organize a workshop with City of London Police and the Economic Development Unit of London Corporation, for a selective audience, on the processes necessary for co-operation in investigating cases that are outside normal policing priorities.**
- **exercises to make the business case for action and to secure the necessary political support/priority for e-security and crime prevention.**
- **request that Home Office organize and fund an exercise on how routines for co-operation between law enforcement and industry might be established, so that pilots can be operated within agreed frameworks with law enforcement adequately resourced to handle their side of the co-operation.**
- **Work with the Jill Dando Institute, Skills for Justice and others to update EURIM survey of University activities to facilitate the growth of trusted support and skills networks.**

## **1. Review of paper on scenarios**

1.1 The EURIM meeting with Paul Goggins on 18 July discussed the need for improved cooperation between law enforcement and industry in view of the limited resources available to law enforcement. A paper circulated with the email carrying the invitation to this meeting, summarized possible scenarios for co-operation, the skills and processes needed and the issues to be addressed. One aim of the meeting was to identify any omissions from the paper.

1.2 Political priority is focused strongly on extreme pornography on the Internet, driven largely by the fears and concerns of MPs' constituents. However, some MPs are showing increasing concern about end-user vulnerability in general.

1.3 Industry priorities vary, with one focus on online vulnerabilities, low-level crime reduction and prevention, and another on fraud and other attacks that cost big business significant amounts of money. However, like other white-collar crime, this tends to be a lower priority for law enforcement, and so industry has to defend itself. The e-Crime Group meeting on 15 September agreed clear actions on education and online vulnerability. Several members of the EURIM e-Crime Group are also expected to be invited to cross-departmental activities now being planned with regard to electronic and on-line security across Government.

1.4 EURIM has volunteered to try to provide Home Office with information as to what industry might reasonably be expected to contribute in cooperation with law enforcement, in which areas of operation, the nature of any constraints, and how we might balance political, law enforcement and industry priorities. This should aid ministers in drawing up a UK strategy for public announcement to an international audience in November.

1.5 It is recognised that offline crime usually has a counterpart or component in the online world; however Industry's current concern is large-scale, serious organised crime and money-laundering, electronic or otherwise, rather than identity theft. Law enforcement can maximize its efforts by exploiting freely-offered corporate resources and expertise in investigations, but needs to establish routines in order to be able to make requests for assistance in the first place.

1.6 Law enforcement generally does not have the resources for cross-border, multi-jurisdictional investigations of crimes against business, unless they fit local policing priorities. However, the City of London police will prioritise large scale fraud and cases that threaten to cause economic damage to UK plc, especially where business is willing and able to fund key aspects of investigations. It is thus possible to organise international cooperation to combat e.g. networked software piracy by penetrating pirate networks at a strategic level. The examples given involved co-ordination with the City of London force and with foreign law enforcement agencies from different continents, and deploying appropriate evidence-gathering procedures and forensics in mounting successful operations to protect a company's revenue, reputation and image.

1.7 Software piracy is an attractive and lucrative target for organised crime. As NHTCU morphs into SOCA, it will become more internationally-oriented and concerned with UK plc, and so is likely to try to disrupt and dismantle such operations. A long-term strategic approach involves working with customers to identify software thieves and their distribution networks, then providing intelligence free to law enforcement. Infiltration of bid teams bidding for outsourcing projects is another concern to large organisations where information has to be protected from both physical and electronic penetration.

1.8 American-owned companies would generally respond positively to requests for immediate help from UK law enforcement (e.g. technical advice), but more complicated issues would be passed to the company legal arm in the USA. There is no obligation on the company to go beyond offering help to law enforcement, responding positively only if it is requested.

1.9 Local forces still tend to concentrate on the contents of a computer's hard drive rather than networks, because local forces have the resources only to focus on local priorities (although the City of London force has access to greater resources). Industry responses should be tailored to the assistance the local force would like. The West Midlands force is trying to reach out to the SME community through its local WARP (Warning, Advice and Reporting Point).

1.10 While the Group's remit is to find out what the industry can do for law enforcement, it was not simply a case of asking what law enforcement requires. It was pointed out that responses to force needs could not be made until priorities were set. In addition, law enforcement needs industry help

with resetting the political priorities so that adequate resources are available. Although fraud costs the country £billions, it had not become a priority because it fell between local and national criteria. However, Internet fraud was not on the same scale. It was suggested that IoD should be able to raise the priority of fraud as a national issue through its network of members and activities.

1.11 It was doubted that even the Metropolitan Police had sufficient resources to tackle computer crime. Since the strains caused by Operation Ore, and more particularly the war on terrorism, forensic and computer specialists are often permanently 'borrowed' by the security services or attracted to the private sector, and as soon as new people were trained up, they are lost to the industry or 'spooks'. However, this was an old problem, and some people did eventually return from industry or other operations.

1.12 All police forces are overloaded, and none have the capacity to handle 'new business' and engage in proactive policing with respect to computer related crime. Although the SFO has its own investigators, there are additional legal and accountancy advice costs that limit the annual number of cases that can be handled. There is no budget for extra officers and no capacity to respond to industry offers of help – unless most of the work was done and resourced by a corporate. Individuals might also wish to volunteer without the backing of their company, and there may be a pool of potential industry volunteers with skills outside their normal work that could be used by the police (e.g. those who enjoyed practising relevant technical skills that are no longer part of their current job). However, while this pool may exist, its size is unknown, and those with skills may not have updated them.

1.13 While the police are experienced in forensics and do not need advice here, they do need extra resources. Law enforcement needs to know what industry can provide in line with local and national priorities, but divisional commanders have to focus on their own remit, so industry is unable to convince the police that it can help, unless the police approach the industry. This presents a Catch 22 situation with industry having different priorities, which can only be addressed if a corporate resources its own investigation to the point where it has to hand over to a legal power for prosecution.

1.14 The Get Safe Online initiative will need to be properly resourced so as to handle the queries that will be generated if the awareness campaign succeeds. There is an urgent need to make the business case for additional resource from government as well as industry. This is best done via IoD or CBI to Home Office, DTI and/or Treasury.

1.15 Serious international crime that doesn't fit police priorities may be adopted by the City of London police, *especially if* business provides the resource. On the other hand, tackling local crime may be suitable for trained industry volunteers. Between the two is the SOCA remit, where national contacts should be available, with set routines in place. The proposed regionalisation of fraud squads should help in reducing local force 'ownership' claims. However, the Group should not recommend 'sticking plaster' solutions to problems at national level, where Government should be putting in more resources.

1.16 Neither is it EURIM's role to solve law enforcement's problems, but to provide a platform for offering industry's assistance. Offers of assistance have been made and it is up to the police to accept. It was suggested that we need to prove that the concept works by running pilots at force level, defining the resources and skills needed, and how industry can provide them. If successful, the model can be offered more generally. Successful pilots run by a company might well be publicised and organisations can become involved if they wish, but it was not the company's job to 'sell' the pilot.

1.17 A company, as part of its Corporate Social Responsibility (CSR) approach, will ask for volunteers for a particular task; the key point is that a clearly-defined request for assistance should be made by law enforcement prior to sending out a trawl for volunteers. It is not up to industry to ask the police what they want. Most major companies, and law enforcement agencies, hold a skills matrix, which allows rapid matching of skills required with people possessing those skills. The police already know what skills are needed in a particular case. A good choice for a pilot would be a simple crime-prevention package, which could be put out rapidly to give value to police forces.

1.19 EURIM, as agreed with Paul Goggins, should be aiming to change the political climate and therefore budget constraints. A clear point of leverage in pressing for political priority would be the proposed 1:1 meetings with individual MPs on security and crime prevention for their own systems. This would address related issues of identity theft and botnets, broadening out to the threat to UK plc.

1.20 The only current mandatory training for MPs is 30 minutes on how to use the connection; many delegate this to their assistants. EURIM's IT officer has provided IT support for a number of Labour MPs (and Cabinet Members) and might also help press the case for improved security training.

## **2. Discussion and Actions**

### **2.1 The agreed actions can be summarized as:**

- 1) help organise pilots on crime prevention in the Thames Valley area and West Midlands Digital Advantage, tied to GSOL messages;**
- 2) EURIM to focus on changing the political climate so that law enforcement is better resourced and able to ask industry for the assistance it needs;**
- 3) organize a workshop with City of London Police and the Economic Development Unit of London Corporation, for a selective audience, on the processes necessary for co-operation in investigating cases that are outside normal policing priorities.**
- 4) exercises to harness political support to gain priority for e-security/crime prevention.**

2.2 ACE Insurance is offering a new 'cyber-insurance' product based on sound statistical data and modelling. This may be useful compared with the 'fudgy' data available on 'cost of crime to business'.

2.3 Regarding the Thames Valley Police pilots, CS has contacts at the operational level and will explore these. This should include the current as well as retired IT community. Some universities had collaborative programmes with police forces, and can supply training and expertise to individuals in gathering evidence etc.

2.4 Work has been done with the Conference of Professors and Heads of Computer Science on identifying computer forensic courses in UK universities, in particular which universities were linked to local police forces. Money was being made available for initiatives, e.g. PITO money channelled into the Engineering Department of Sheffield University. One of the outcomes had showed that the parties wanted to network with each other, **and so an update exercise on this might be useful.**

2.5 **Such an exercise should be linked with the Jill Dando Institute Crime Science network, Skills for Justice, Fred Piper's work at Royal Holloway and the Experian validation and accreditation exercise (VALUE) to establish a trusted network of skilled, qualified and vetted individuals available for forensic support.** However, a sponsor is needed to maintain current vetting; a number of people in the City have had very high security clearances, and may be willing to be brought up to date so that they can have clearance to volunteer to work in a particular field.

2.6 An opinion was expressed that skilled and vetted volunteers on a list might become disillusioned if not engaged in some meaningful exercise – who would use them? How would a company react to their use? What are the credentials? What about the legal aspects? The 'Business Link' initiative of the 1980s had proved to be an unfortunate example, in which the advisers used were not up to date with training, vetting and subject matter, and consequently gave the wrong advice.

2.7 There was a view that few parts of law enforcement were in a position to put up-front resource into collaborative initiative with industry and it was recognized that Home Office would need to evaluate any proposals. Successful prosecutions of crimes are unlikely unless it is possible to operate and track forensically along the means of communication used to perpetrate the crime. The CPS therefore needs the appropriate level of up-to-date high-tech skills available. **It was agreed that EURIM officials request HO organize and fund an exercise on how routines for co-operation between law enforcement and industry might be established, so that pilots can be operated within agreed frameworks and evaluated for possible scaling and replication.**

2.8 Chris Sundt's paper represents the base draft for Home Office support for any projects. This should include a set of proposals that industry is able to say it can deliver when HO asks for them. We should therefore fill in any gaps in CS's paper, and undertake exercises to make the business case for action and secure political support and priority.