



**Draft minutes of the E-Crime Group meeting, 15 December 2005, 1400-1600 hours,  
Room W1, Westminster Hall**

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

**1. Review of e-Crime Group progress and plans**

1.1 Following introductions around the table, a summary of progress to date was given, with current issues and forward plans for the EURIM e-Crime Group.

RIPA III

1.2 Plans for a consultation on the implementation of RIPA III were announced at the Home Office Industry Forum and the Internet Crime Forum. EURIM has organised a closed, pre-consultation workshop on 11 January 2006, to discuss concerns that the RIPA III legislation will apply to those involved with international financial services. If true, this could cause those unwilling to give similar access to overseas governments to move operations out of London (the cost of which to the UK economy has been estimated at £' tens of millions or £' tens of billions, depending on who you talk to. A subsequent open event would be organised as soon as the main HO consultation starts. The aim is to structure the subsequent consultation to avoid unnecessary controversy and embarrassment by removing unintended side-effects.

IT Security Skills

1.3 The Security Industry Training Organisation (SITO) proclaim on their website that "the key sub-sectors that Skills for Security will initially cover are: Access Control Systems Installation ... Dog Handling, Door Supervision, CCTV Operation (Public Space Surveillance), CCTV Systems installation ... IP Security (Electronic), IT Security...Risk Management ... Security Consultancy, Security Management and Security Guarding'.

1.4 However, Skills for Security is not a Sector Skills Council in the Skills for Business Network, but a new standards-setting body set up to service the Security Industry Authority under the chairmanship of Lord Stevens of Kirkwhelpington. There are issues of responsibility, and Skills for Justice (S4J) is said to be discussing demarcations with Skills for Security in the criminal justice area. We are also discussing a draft parliamentary question to confirm who is responsible for occupational standards in this area, once it is confirmed that the answer will be the relevant Sector Skills Councils (S4J and E-Skills).

1.5 The S4J steering group is looking at the issues of moving from standards (once these are developed) to courses and qualifications. A meeting has also been organised with e-Skills, who are working on ITQ (IT user National Vocational Qualification; <http://www.e-skills.com/itq>). ITQ forms part of the new Apprenticeship Framework for IT Users and will bring together the various qualifications in a common framework.

1.6 The qualifications offered do not as yet include e-security or Internet safety; even the ECDL security coursework is minimal and testing for it is not mandatory. However, ITQ offers the opportunity to make these mandatory; the discussion with e-Skills will include how to identify, recruit and involve appropriate employers, with those responsible seeing this as a good opportunity to increase industry involvement.

1.7 How this fits with the Institute of Information Security may depend on what INSTIS wants its own role to be. At the '7799 Goes Global' conference (12 December), the main concept seemed to be to raise the reputation of IS professionals, and ensure that there are clear standards of competence and mentoring processes in place.

1.8 As yet there appears to be no common source of information in this area, and much incomplete, inconsistent and confusing data. One of the aims of INSTIS is to create a central point of reference for assessing the value and validity of courses, and agreeing which would count towards qualification criteria. It is hoped that the current developments will act as a catalyst for changes in the way that information security professionals are regarded.

1.9 Greenwich University is targeting to be a local training and professional updating centre for those working in Canary Wharf (a couple of stops on the DLR) and also to help the Conference of Professors and Heads of Computing and others, to facilitate improved networking across those who provide Infosec and Forensic MSc's, research and training, and support services to their local police forces. These are often handled by the same people but at different levels of security and trust. There are a number of groups, all with varying awareness of and relations to each other. An extension and update of the matrix produced by EURIM last year would be most useful, and unless this is already being produced (e.g. as part of the preparatory work for INSTIS) we should seek to organise and/or fund this

1.10 It is uncertain how far the various players can actually be brought together given the wide range of groups, including those with no wish to talk to others, even where they know of their existence. It was suggested that the Government Protective Marking Scheme could help. The GPMS, with four levels of protective marking (from 'restricted' to 'top secret'), provides a common baseline for safeguarding information, particularly when it is shared by different organisations. The higher the level of protective marking, the stronger the security measures used to protect the item.

1.11 However, this assumes a hierarchy, whereas we are actually dealing with a series of rings, and different types of trust within each ring (e.g. 'I trust him with my life, but not with my wife or my money!'). Most models deal with strict banding rather than inferential security, which implies that a picture can be pieced together by assembling separate bits of information. Protective marking and flagging of individual items can develop into a complex problem. Strict banding does not work in a networking environment. A deal of work remained to be done at different levels, and a major aim should be simply to ensure that, as far as practical and desirable, the various groupings knew of each others existence, if not necessarily all that each other was doing.

1.12 The current activity of the SIA in regulating their security consultants should be monitored. The SIA had distributed a series of questionnaires as part of the Private Investigation consultation process, with a return deadline of 5 December 2005. However, the questions do not appear to reflect a full appreciation of the issues. The basic problem is that the Private Security Industry Act 2001 defines security too loosely. S4J also have accreditation responsibilities for a number of roles and jobs within the criminal justice system.

1.13 The Crown Prosecution Service had recognised that the importance of the role of 'disclosure officer' meant that it should be accredited, but this could take a year to organise through training courses. Monitoring, updating and evaluation also need to be ongoing, so a deal of work is involved. This was a concern with the SIA, where wheel-clampers and bouncers were licensed after a 5-day course, with no follow-up. Such a procedure for security consultants is likely to create a false sense of security because competency could not be guaranteed.

1.14 Some 95% of students on InfoSec courses at Plymouth University are foreign. If this trend is typical, not enough students from the UK are being trained to be able to deal with industry demand. At the same time, around 4000 InfoSec students per year are qualifying from Indian universities, and are probably extremely competent. The problem could be attributed to career development – there is no apparent career advantage in attending courses, and an incentive is needed. However, this may be changing, and INSTIS is trying to develop an environment of professionalism that will be seen as worthwhile.

1.15 Greenwich University is looking at trying to offer all ICT students the opportunity to achieve CISSP (Certified Information Systems Security Professional) and other security qualifications as part of mainstream courses, whilst acting as the training and updating centre of choice for those working nearby (e.g. in Canary Wharf) whose companies expect them to hold and maintain the American qualifications (as opposed to inventing new qualifications).

### Confidence in public sector information security

1.16 Confidence in the handling of security and identity is a pre-requisite for the successful implementation of the Transformational Government strategy. Secure data sharing initiatives are springing up across the sector, and the EURIM Personal Identity Group is compiling a grid of these, with an objective of distilling examples of good practice. Another aim is to try to change the attitudes of number of departments that do not follow good practice as a matter of routine, including by priming backbench MPs to ask pertinent questions in Parliament.

1.17 The difficulties of achieving action in this area should not be underestimated, and it has been suggested that EURIM should not shy away from controversy, provided this has an agreed and constructive objective. **There is a need to discuss the setting up of a separate subgroup within the EURIM e-Crime Group to deal with this set of issues, and look at how this links with the set of tasks within the remit of the new cross-departmental networking group on security research**

### Get Safe Online

1.18 The plans to integrate IT Safe with GSOL are most welcome, but what happens to GSOL after 1 April when NHTCU comes under SOCA, which does not have a publicity remit? Who will "own" the campaign? What are the plans, if any, to ensure that Government, as the UK's largest employer, plays its part alongside the growing plans of private sector employers to run awareness and training programmes for all staff and customers? Has any thought been given to the role of the trades unions, many of whom regularly send magazines to all members which could carry appropriate material and links. PV agreed to contact Amicus on this.

1.19 It was suggested that the next EURIM newsletter include a call to members to raise the future of GSOL politically, but first we should agree some positive suggestions as to what should happen. Should we call on HO to provide funds to the Metropolitan Police, so that they can host GSOL on behalf of ACPO? So far Government had contributed only £150,000 alongside similar contributions from each of 9 private sector sponsors, mainly to build the infrastructure. Sponsors had also contributed posters, leaflets and roadshows to help launch an ongoing 2-3 year campaign which had already shown great success in reaching audiences that other campaigns have not, for example the over 55s. However, a recent survey showed that although a majority of SME's use broadband, very few accept payment over the Internet because of lack of confidence that they will not be hit by charge-backs (not commonly included in reports of on-line fraud). The Forrester-BSA survey "Understanding Consumers' Internet Security Fears" [www.bsa.org/uk/upload/Forrester%20BSA%20GB%20final.pdf](http://www.bsa.org/uk/upload/Forrester%20BSA%20GB%20final.pdf) also indicates there is much still to be done.

1.20 What should the EURIM e-Crime Group be calling for with regard to what individual departments and agencies are doing to promote security, consistent with the Government's aim to foster confidence in the Internet? We need to point out that the Transformational Government agenda depends on take-up online by the public.

**1.21 A EURIM meeting in February could be held in advance of the NHTCU Congress, designed to bring together the target audiences at which EURIM members would suggest specific actions to Government, for follow-up by the industry.**

**1.22 The idea of a WARP (Warning, Advice and Reporting Point) for the Palace of Westminster and MPs had been proposed and the planning and launch of this could provide an excellent vehicle not only for educating MPs regarding their own security but also for involving them in giving higher priority to overall action in this area.**

### Crime Prevention Co-operation

1.23 There are 3 crime prevention and reduction pilots of interest to the Group: Advantage West Midlands RDA, the Community Safety Team based at Maidenhead Police Station and the Yorkshire Forward bids for EU funding for a major exercise. There are practical problems in the operation of the pilots, particularly regarding legal and regulatory constraints around investigations where active cooperation with industry is desirable.

1.24 WM Police have been aware of the need to integrate crime prevention and reduction into their operations, and have secured resource to establish an e-crime prevention centre in collaboration with Wolverhampton University and local authorities (involving SOCITM and LGA), and aimed at local industry. They are also in contact with NISCC to develop a local WARP, and have identified key areas for industry to help through skills and resource (e.g. help hosting and maintaining a website).

1.25 A report by PRCI consultants on the effects of e-crime in the area had made many good recommendations for adoption by Advantage West Midlands, including setting up a support centre, and crime prevention awareness, education and support activities to help attract and foster new business. Unfortunately, the consultants to the RDA appeared to believe that action in this area was the responsibility of central government, not the RDA. **There is a need for rapid political action to remove this obstacle.**

1.26 The 'Maidenhead pilot' is the electronic security equivalent of a mobile crime prevention officer (the Berkshire bobby) who can visit homes in the neighbourhood to give practical advice and help, and fix simple e-problems. Work with the CSO is progressing to bring in local expertise.

1.27 A progress report on the pilots would be useful to support an approach to Home Office on the need to provide funding and support to document and monitor pilots in order to be able to replicate them elsewhere. There is also a need to use the pilots to promote and test linkage between the GSOL exercise and local police crime prevention efforts.

1.28 The pilots are likely to be ready for launch towards the end of Quarter 1 of 2006, and we should be planning a meeting with the minister in April (after the High Tech Crime Congress, unless brought forward and linked to it). He would then talk about what Government would like to see happening in partnership with industry, including how to ensure the future of GSOL. Senior Industry speakers would be asked to respond with an account of what they had done, and invite others to join them. MPs and officials from the various departments and agencies whose support is needed to make a reality of any cross-departmental policy would also be invited.

1.29 SEEDA (South East of England Development Agency), is AWM's counterpart in SE England. A new Security Knowledge and Innovation Network (Security KIN) is being developed, led by Cranfield University with funding from SEEDA to encourage companies in the security sector to work with security end users, technology specialists and universities in developing innovative new products and services. It aims to clarify the business case for security solutions; focus on the integration of security solutions in practice; take a proactive approach to designing future security solutions; and support collaborative research relationships, funding bids and projects seeking to acquire and develop relevant security solutions. The network is being coordinated by Paul Osborne at Cranfield University's Campus at Shrivenham in Oxfordshire and has the backing of leading security industry organisations (QinetiQ, SIRA, Thales, BSIA, APPSS, iAfB). It is engaging with relevant expertise in regional universities (Royal Holloway, Surrey, Southampton and Kent) and key end users (Police, Home Office). PO can be contacted on 01793 785004 or [p.g.osborne@cranfield.ac.uk](mailto:p.g.osborne@cranfield.ac.uk)

1.30 A document by 'reporters without frontiers', which advises on how to be both secure and anonymous, may be of interest: [http://www.rsf.org/rubrique.php3?id\\_rubrique=542](http://www.rsf.org/rubrique.php3?id_rubrique=542)

#### Investigatory Co-operation

1.31 A workshop has been organised 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. The format and content of the workshop will be based on a major international investigation into software piracy led by Andy Clarkson of IBM with the City Police. The victim was a French company, highlighting London's reputation in this field and the importance of such work in positioning London as a global centre for Internet Policing and Governance, alongside its similar role with regard to maritime piracy and other forms of global disputes resolution (said be worth over £30 billion a year to the UK economy).

1.32 The target audience is the heads of security of senior financial service organisations in London. Issues covered will include the international cooperation protocols, procedures and financial responsibility involved in persuading a police force to undertake a major, costly international investigation, and how this might be repeated elsewhere. The City of London Police is the only force where tackling fraud and economic damage to London and the UK is a key performance indicator.

#### Good Practice in reducing overall vulnerabilities

1.33 Action to discover the current state of play on end-over-end authentication of traffic, what is practical and possible etc. should involve Nominet (now a EURIM associate member) who have much the best circulation lists of those who will need to be consulted. This would be a tricky exercise; debate has moved on over the last few months and what was considered impossible 18 months ago is now being done. It would be useful to build on discussions with John Thompson (CEO, Symantec), in the

context of online banking and transactions. Issues to discuss might include the way in which products are set up to enable secure authentication, who can assist and how. What is good practice, and how do you secure adoption?

#### Good Practice in protecting those at most risk

1.34 Much progress has been made recently with regard to child protection, culminating in a series of announcements in November, including good practice guidelines and the new agency that will come into being on 1 April. There was some doubt about whether or not the previously planned workshop to bring together the electronic security, child-care and education professionals on this would still be useful in advancing understanding and cooperation. This needs to be discussed with those concerned.

#### Securing Informed Political Support

1.35 The planning and creation of a WARP for MPs might well be the best point of leverage. All MPs were provided with online facilities, but not all use them. This might be related to an aversion to the technology, or in other cases the volume of emails received in their inboxes. Usage by MPs is influenced by a number of factors, and response times vary enormously!

1.36 Plans to announce a national Strategy for addressing computer assisted crime have continued to slip as priority is given to the setting up of a new child protection agency. This is being created in parallel with SOCA, and there is a clear implication that the rest of e-Crime is a low priority at present. Resource had been overwhelmed by demands both centrally and locally to investigate child pornography; a focused unit might be a better vehicle for controlling the allocation of resource. Crime reporting was also an issue, because current practice does not identify the nature of a crime or its victims! With no searchable database, how can an assessment be made of the success or otherwise of initiatives against e-crime?

1.37 There was a concern that the formation of SOCA and the new Child Protection Unit could lead to a cessation of activity on other forms of computer related crime, hence the need for political pressure to ensure the announcement of new home for GSOL and scaled up government support before March 31<sup>st</sup>.

## **2. Action plans**

2.1 Revise and publish a paper on 'Making the Internet Safer', retitled, expanded, edited, with updated recommendations and a section on current threats and vulnerabilities - this should cover the actions necessary to address the apparent backlash against doing business online because of the fear of fraud, identity theft etc.

The most recent survey by the Oxford Internet Institute showed that 8% of those interviewed had stopped using the Internet over the past year (c.f. 6% in 2003); barely 1% cited 'an unfortunate experience' (as opposed to no value, too difficult etc.). Other more recent surveys are, however, indicating that fear of fraud was indeed inhibiting the rise of internet banking and use of the Internet for high value transactions (as opposed to bookings and discretionary spend).

It was agreed that the paper should include an updated section on reporting. Issues might include whether reported data is for regulatory or criminal purposes, how reporting procedures should be structured etc. If there is no clear purpose to reporting, why should people spend time and effort on it?

2.2 Help launch and recruit support for replicable crime prevention pilots – work was continuing, and we should target a progress report for Home Office in March, hopefully leading to a Home Office contribution and the announcements of links from the pilots to the follow-on to GSOL.

2.3 Produce and promote updated political briefing material - ideally this should be done in the context of the creation of a WARP for MPs. Approach NISSC and Cabinet office to discuss how this proposal should be progressed.

2.4 Workshop on co-operation on large scale investigations - date to be arranged.

2.5 Co-operation with Skills for Justice and E-Skills - PV will meet with e-Skills to line up plans for networking and cooperation. Consultation with the planned DTI security research network and others is also desirable to ensure effective networking and/or the creation and updating of a grid of who is currently doing what.

2.6 Ministerial meeting to announce 'Partnership Policing' plans, building on and welcoming practical examples of co-operation – possibly in February, to recruit support for the pilots and provide a platform for announcing the future home of GSOL. Contact HO to discuss possible timing.

2.7 Identifying MPs in the AWM geographical boundary – DW to action.

2.8 RIPA workshop with international financial services players set for 11<sup>th</sup> January. Further action is to be decided in the light of the outcomes of that event.