



**Summary report of the E-Crime plenary meeting, 15 September 2005, 1000-1200 hours at
British Computer Society offices, 5 Southampton Street, WC2**

Chairman: Philip Virgo (EURIM);

Rapporteur: Dave Wright (EURIM)

SUMMARY OF MAIN POINTS

1. The EURIM meeting with Paul Goggins on 18 July agreed an agenda to identify and prioritize the issues and messages that should be included in an education programme for MPs, and to determine the nature and scale of support HO can realistically expect from the industry.
2. Political interest in e-crime is now focused on the Home Office consultation on possession of extreme pornographic material. However, a major objective of the members of the EURIM E-Crime group is to secure political priority for education, skills and systems security in schools, and to do this without alarming customers.
3. Large scale identity theft using botnets (by phishing, sniffing, keylogging and other bogus emails) is linked to the recent rapid increase in broadband take-up in the UK, which now has more 'botnets' than the USA. A major difference is in the different approach in the USA, where ISPs are under greater pressure to provide more protection to users. Security provision and awareness levels in the UK are generally inadequate. Phishing and botnets are increasingly used by organized crime on a scale that is beginning to undermine trust in e-commerce and Internet transactions.
4. Identity theft is a political priority for Home Office, particularly in relation to forthcoming identity card legislation, and the area of financial e-crime. **It was agreed to produce a paper to inform MPs of the link between the large number of botnets and organised crime in the UK compared with the USA, and to persuade them that the consequent damage to the UK economy requires greater political priority be given to broadband security, with increased co-operation from ISPs.**
5. **Symantec CEO John Thompson will address a EURIM discussion dinner for MPs and Ministers in London on 2 November.** The talk will discuss political and practical solutions to identity theft, the different approaches in the US and UK to Internet safety and security, and possible responses from government and industry.
6. The EURIM aim is to seek to persuade MPs to press Government for law enforcement to be given significantly more resources to combat computer assisted crime in general. There is also likely to be more benefit in crime reduction and prevention rather than in investigative initiatives.
7. A major **Internet security awareness campaign** is due for launch in Quarter 4 targeted at online consumers and micro businesses - two of the most vulnerable groups of users whose computers can subsequently be used as zombies in botnet attacks. For more information see: http://www.nhtcu.org/nqcontent.cfm?a_id=12451&tt=nhtcu
8. Evidence from personal experience and from MPs' postbags indicates that it is vitally important for practical instruction to accompany any educational programme, with follow-up evaluation exercises, otherwise the advice may not be implemented due to lack of user understanding, confidence and/or skills.

1. Review of EURIM E-Crime Progress Report

1.1 A main aim of the meeting was to review the EURIM E-Crime Group progress report circulated in advance of the meeting. The Group had produced over 50 recommendations since April 2002, in addition to the paper calling for a national strategy on e-crime in collaboration with the then minister, Bob Ainsworth. Agreement had been achieved on all those measures within the Home Office remit that attracted no cost and did not require legislative time. Unfortunately, the launch of the strategy has subsequently slipped, and most of the remaining recommendations cost new money, cut across departments, or require legislation.

1.2 The progress report lists the Group's recommendations, the official responses (if any), and subsequent actions. However, political interest is now focused on the Home Office consultation on possession of extreme pornographic material, and it is therefore important to 'educate' MPs and their researchers. The content of any briefing we produce should aim to ensure that any outcome is reasonably workable and not counterproductive. Another major objective is to try to get political priority for e.g. skills needs, and education and security in schools.

1.3 The meeting with Paul Goggins on 18 July focused on the issue of potential Home Office partners for pilot programmes. An important action to emanate from the meeting was for EURIM to work with Home Office on identifying which messages should be included in an education programme for MPs, in order to decide which issues should be prioritised. Another issue is the amount of support HO can realistically expect from the industry, and in which areas (as opposed to what is desirable, but without resources to deliver).

2. Review and discussion of priorities for action and who will assist

2.1 The scale and importance of online identity theft, and its use in organised crime, has not been fully recognised. The Symantec Internet Threat Report for release on 19 September shows for the second consecutive 6-monthly period, that the UK has the largest proportion of zombies (systems hijacked for use in botnets) in the world. That proportion is higher than in nations which have had broadband for longer (e.g. US or Sweden) implying a linkage between the recent rapid expansion of broadband in the UK and the proliferation of botnets, probably caused by neglecting security concerns regarding the home and small business user. This is a critical message for politicians, because botnets are the means of launching distributed denial of service, sniffing, keylogging, spam and phishing attacks, and can also host multiple fake websites pretending to be Ebay, PayPal, or a bank, and harvest personal information. All undermine confidence in e-commerce and online transactions.

2.2 The legal framework was of less concern than the fact that the UK has more botnets than the USA. This probably reflected effective ingress and egress filtering by ISPs in the US, brought about by political pressure, which was not in place in the UK. It is therefore a question of applying similar pressure for increased security here.

2.3 The ministerial priority is to deal with extreme pornography in response to strong, constituency-driven demands for political action. Any other issue is unlikely to raise the same degree of interest, although a number of MPs have been the victim of phishing and spoofing attacks, and have concerns about the activities of their own children over the Internet. While some MPs are disturbed about wider Internet misuse they receive no coherent message and little practical advice on what can be done, and there is no steer from Home Office. The message from ISPs is generally that the wider issues are too difficult to deal with and users should rely on a firewall and anti-virus software. A better-informed, better educated nucleus of MPs might thus be persuaded to support an agenda that can better address the wider issues.

2.4 A draft brief on security intended for MPs had invited significant criticism because it failed to address the problems faced by the average home user and small business in the practical implementation of the advice given. However, a brief on security for MPs, backed up by volunteers offering practical support in the MP's office, remains a EURIM priority. This route, including labour-intensive 1:1 support as well as briefing, needs to be planned and resourced, and is being considered with ISSA; however, it is essential to have a common set of messages.

2.5 A complicating issue is the lack of evidence for e-crime related to police reporting procedures: cases of identity theft are generally not recorded because there is no mechanism to do so. The use of computers in mainstream crime is not recorded other than as notes. Crimes against business are not

always distinguished from those against individuals (e.g. a burglary is burglary whether it is an office, workshop or home). Most policy is not evidence-based, but is reaction to well-publicised anecdote (e.g. the Australian co-regulation legislation is based on the need to gain the support of a single MP for a key vote). Although it may be difficult to excite MPs about a new issue if it is not directly related to their potential re-election, it may be useful to hook educational messages to MPs' briefings on Internet safety, while victims of identity theft might be encouraged to write to their MP to raise awareness of the problem. The constituency-based write-in is a very powerful tool: ministerial support for the original FAST Bill to extend copyright legislation to cover computer software was the result of only 26 letters to a department that had never faced a write-in before.

2.6 A potentially more serious threat to the country was terrorism and organised crime *per se*. Threats to businesses were considered more important than to consumers, but perhaps the Group should not necessarily consider the biggest threat facing the country, but the biggest threat that we can do something about, in terms of being able to raise political priority. In terms of e-crime, identity theft is highly significant because it provides the means by which organised crime effects money laundering, using 'stolen' identities to set up false bank accounts etc.

2.7 Identity theft is a political priority for Home Office, particularly in relation to the introduction of identity card legislation, and the area of financial e-crime. The choice of a tag may be critical, because associating identity theft with terrorism could divert attention from the scale of e-crime. Identity theft can also lead to the erosion of trust. The user has traditionally had to prove identity to the e-business vendor. Phishing and spoofing attacks have necessitated the reversal of this process, undermining the basis for e-commerce.

2.8 While MPs understood what was meant by the term 'phishing', it was not clear that they were familiar with the concept of 'botnets'. One way to emphasise the seriousness of the problem of botnets might be to present it to both parliamentarians and the public as a privacy concern, showing that hackers can take control of an individual's computer. A Group paper for MPs on reducing online vulnerabilities could include this and put the issues into context. **It was agreed to draft a short note on the scale and nature of the botnet problem, and the current state of play with regard to solutions, in the context of a paper on 'reducing vulnerabilities'**. This would advise MPs on what they should be doing about security, what they should be calling for, and who should provide it.

2.9 The Group readily accepted an offer from Symantec that their **CEO John Thompson, as a charismatic and influential speaker, address a discussion dinner with Ministers and MPs on the issue of political solutions to identity theft**. This fits well with the EURIM forward programme of meetings with Ministers and their officials, Chief Executives, Select Committee Chairmen, officers of relevant all-party groups and MPs, to discuss priorities for political action.

2.10 There is sometimes a sense that when a corporate speaker addresses MPs, they believed they were hearing a marketing speech, whereas a talk on the same subject, but from a law enforcement viewpoint, produced a different reaction. John Thompson would have the advantage of being able to talk to politicians as an appointee to the National Infrastructure Advisory Committee. One advantage of an address from a speaker at CEO level was that suppliers could be quoted, on the record, and held to account for what they undertook to deliver, or said was deliverable.

2.11 Raising awareness of security problems may have the effect of scaring users unless accompanied by practical solutions. This E-Crime Group should address the issue of providing credible and practical solutions before running awareness exercises, and focusing on prevention rather than enforcement. This might best be addressed nationally through the ISPs as the gateway, either by self-regulation under increased political pressure, or through a more prescriptive approach.

2.12 The usual EURIM aim is to seek to influence MPs, because of the need for new and/or better legislation, and because they are able to exercise some influence over budget allocation and political priorities. The latter is probably more important at the moment, because the calls for action require money to be spent. There is likely to be more benefit in crime reduction and prevention rather than in investigative initiatives. Frustration was expressed that the achievements of the Group in producing targeted papers, and in calling for the establishment of what became Project Endurance, had yet to translate into discernible changes in behaviour.

2.13 The differing views of DTI and HO were also a cause of conflict, often getting in the way of practical progress. Thus HO will advise on the need for security, while DTI will advocate the benefits

achievable through computer technology; there needs to be a more unified approach. EURIM should identify small projects in which incremental advances towards a well-defined goal are achievable. Building on the published papers that set the scene, our next short-term objectives should be work with MPs to change materially the online security landscape.

2.14 Changes can be achieved – we need to emulate the success of the USA in dealing with botnets and associated crime, and learn the lessons. ISPs need to do more, and it would be best if DTI and HO took a more proactive approach in this. However, ISPs are split between and within themselves. The security, regulatory and marketing sections each have a different view, and while marketing to corporate customers is beginning to emphasise security rather than price, the regulatory advice approach is to avoid responsibility. A note explaining why the UK has the largest botnet problem, and its potential solution, can offer a strong political point of leverage, especially if this can be reinforced by the visit of John Thompson, and with representations to the DTI select committee. HM Treasury is another important point of leverage (but should be targeted via the City).

2.15 The main political aim of the e-Crime Group is to demonstrate what can be done by the combined actions of law enforcement and industry, and to use this to help raise more difficult items up the political agenda via MPs. The priorities for action can be summarized as:

- increased broadband security to combat identity theft;
- budgets and funding priorities, focusing on e-crime and vulnerability reduction and prevention;
- legal issues, e.g. the CMA, DPA (issues around Operation Glade), where there appears to be agreement that action is needed, but not as a matter of priority. Should the Group press this?

2.16 Amending the CMA did not appear to be a current political priority compared to action on extreme pornography, with a response due to HO by end November, or fraud. While there used to be many concerns about the CMA, the arrestable offence is now e.g. extortion, in which the computer is (mis)used in the commission of a DDOS attack. The CMA is actually quite a robust piece of legislation, though not used much directly, and can be invoked with respect to other offences. Therefore there is no pressing need for amending the CMA (or DPA) to make offences extraditable; the new Fraud Act would cover many of the outstanding issues anyway (although the legacy maximum sentence of 10 years did not reflect the serious nature of the crime, and would not encourage guilty pleas). There is thus no need for the Group to produce a paper on legal issues.

2.17 The meeting was informed of the imminent launch of the **'Get Safe Online' Internet security awareness campaign**, which had Government and private sector support. The campaign, which is the sequel to the 'Project Endurance' Steering Group chaired by ACC Len Hynds will be targeted at online consumers and micro businesses (fewer than 10 employees). These represent two of the most vulnerable groups of users whose computers can subsequently be used as zombies in botnet attacks. It would be useful to draw MPs' attention to the campaign in order to raise its political priority and therefore budget allocation, in order to reduce botnet attacks employed by serious organised crime. For more information see: http://www.nhtcu.org/nqcontent.cfm?a_id=12451&tt=nhtcu

2.18 The meeting was alerted to the gap between the aims of such a campaign, and the ability of users to interpret and implement the advice. Introductory physical support is needed to help users understand e.g. how to update a firewall, and to guide them to further support from professionals. Simply pushing out Internet awareness campaigns is only half the solution; a higher priority for crime prevention is needed to push for more funding.

2.19 Education should be ongoing, with visits to schools, SME's etc., and toolkits. Security should be sold as part of a system, not an optional extra, but we need to be careful not to undermine consumer confidence in the Internet and e-commerce. However, no ISPs or vendors are yet involved. Figures quoted at the OII conference stating that consumer 'switch-off' from the Internet had risen from 6% to 8% - illustrated the need for higher political priority, and funding, for consumer reassurance. The contrast between the USA and the UK should provide a strong point of leverage in persuading ISPs that they need to be more involved.

2.20 The value of discussing Internet safety and extreme pornography is that MPs are already strongly engaged in doing something to combat this through their constituency caseloads. The issue is how to harness this political energy constructively – and one opportunity would be to put Internet safety in schools at the heart of education policy. How then should we involve Industry volunteers in delivering pilot programmes to demonstrate what could/should be done?

2.21 Microsoft and Cisco (and maybe others) had Internet educational programmes prepared for schools from the earliest years, which would represent a new start for a new generation (**there will be a EURIM meeting 6 October on online child protection and Internet safety programmes**). Cisco has 20 CRB-screened volunteers, trained by Childnet, to teach Internet safety, currently in primary schools. Although this may rise to 100, this is unscalable in terms of the education system, and one way forward may be to include it as an updateable subject in the school curriculum, taught by trained teachers.

2.22 The Worshipful Company of Information Technologists, together with the British Computer Society, co-ordinate 'IT4Communities' which brings together the IT and voluntary sectors to facilitate a common approach. There are currently some 2000 volunteers with IT skills involved, with sponsored funding, offering practical ICT support to some 600-700 charities.

2.23 A top priority is the need to persuade MPs to call for a realistic budget for programmes that support the practical implementation of advice from Internet safety awareness campaigns. Evidence from personal experience and from MPs' postbags indicate that it is vitally important for practical instruction to accompany any educational programme, otherwise the advice would not be implemented due to lack of user understanding, confidence and/or skills. Follow-up evaluation exercises might help.

3. Actions

3.1 The key actions from the meeting may be summarized as:

- **A briefing note will be drafted to inform MPs of the link between the large number of botnets and organised crime in the UK compared with the USA, and to persuade them that the consequent damage to the UK economy requires greater political priority be given to broadband security, with increased co-operation from ISPs.** This will be used to help draft the paper on "Reducing On-line Vulnerabilities" paper that was dropped from the EURIM-IPPR study.
- **Symantec will organise a political discussion dinner with Parliamentarians addressed by Symantec CEO John Thompson, with the aim of persuading ministers that practical awareness programmes designed to tackle the threat to e-commerce should be a political priority with a realistic budget.**
- **The briefing note will also be used as input to a paper on 'Reducing Online Vulnerabilities'. We have begun drafting material for this paper. It should include recommendations for action on e-crime prevention and reduction and the need to adequately resource not only awareness activities such as 'Get Safe Online'; but the education, training and support services to enable that awareness to be turned into effective action.**
- **A meeting is being convened on 6th October to discuss what is needed and/or practical vis a vis education programmes.**
- **A workshop will be convened to discuss a programme of 1:1 meetings with MPs (built around helping them and/or their staff on Internet security for their own computer systems). The workshop will aim to bring together players and plan messages, content and resourcing).**

Personal Identity and Authentication are being handled via the EURIM Personal Identity and Data Sharing Group. A meeting to plan the forward programme is scheduled for 29th September.

Subsequent to the meeting Point 2.2 was queried. It was said that UK ISPs risk acquiring civil and criminal liability for traffic across their networks if they do other than act as a 'mere conduit' (by EC directive 2000/31/EC implemented as the Electronic Commerce (EC Directive) Regulations 2002). This was said to act as a disincentive to implement filtering measures, particularly when contrasted with the US situation where ISPs appear to benefit from common carrier status without limitation. This point appears significant and is being followed up.