The Information Society Alliance

EURIM

Parliament and Internet Conference
Thursday 16th October 2008
Report of Workshop D; The UK E-Crime Reduction Partnership

Chair: Rt Hon Alun Michael MP

Rapporteur: Philip Virgo

Participants: Rt Hon David Blunkett MP, Leonard Anderson (SOCTIM), Martin Boyle (Nominet), James Brokenshire MP, Dr Tanya Byron, Jennifer Carlton (Intellect), Andrew Churchill (Telsecure), Les Fraser (Croft Information Security), Robin Gape (BT), Mark Gracey (THUS), Andrew Hardie , Paul Hoare (SOCA), Julian Heathcote Hobbins (FAST), Martin Hoskins (t-mobile), Phil James (Hyder Consulting), Anthony Langan (Samaritans), Annabeth Lange (UNINETT), Emeric Miszti (Tiscali), Dr Vicki Nash (Oxford Internet Institute), Dr David Oswell Goldsmiths College, Jennifer Perry (e-victims.org), Roland Perry, Peter Robbins (IWF), Emily Taylor (Nominet), Richard Tebboth , Nick Thorne (former UK Ambassador to the UN in Geneva), Dan Mount (Office of Alun Michael MP).

The government vision for a national e-crime strategy is of a three-legged stool: the Police Central E-Crime Unit (PCEU), Fraud Authority and e-Crime Reduction Partnership. The council and police are responsible for bringing local communities together to identify the harms they wish to address via geographic crime reduction partnerships. The aim of these is to make the community a safe place as opposed to catching criminals, important though that is. Police respond to criminal acts by seeking to catch the perpetrators. A Partnership's aim is to remove the temptation/opportunity and to create a safe environment.

Over recent months we have been moving from a feeling that we cannot deal with e-Crime because it is too big and complex towards a shared belief that it needs to be addressed by a mix of partnerships, local, regional and international, making effective use of existing legislation rather than calling for new laws.

The time has now come to stop looking at generalities and look at specifics and the EURIM e-Crime Group has found volunteers to lead exercises to look at how the partnership approach might be used to address the concerns of three communities and "make a difference". One the approach has been shown to work it can then be applied elsewhere.

The initial three are:

- The elderly: who are being brought on-line, including by initiatives such as Ruralnet, thus combating isolation, easing contact with grandchildren, etc., but can be vulnerable to fraud and are often fearful.

- Schools: where cyberbullying and stalking, including of young teachers by older pupils, are major concerns.
- Small Firms: where there are a number of initiatives on which to build, but there is often a lack of security and IT capacity.

There is buy-in across Government (Home Office, Cabinet Office, Department for Business, Attorney General etc.) but geographic partnerships engage local businesses (who benefit through more foot-fall in their shopping malls, safer industrial estates or higher property values). The bigger issue is whether those businesses which depend on confidence in the on-line world will see the commercial benefit of engaging through their mainstream marketing and social responsibility drivers, and not just through the security budget.

The Internet Service Providers, Telcos and Mobile Operators sometimes feel that they are a sort of piggy-in-middle. Their customers include both the victims and perpetrators and they themselves are regular victims of fraud and abuse. Even ISPs with multi-million pound turnovers have been driven out of business in the course of major service attacks – with no recourse and no prosecution.

The monitoring and quality control services give ISPs much information about what is happening but they have major problems in passing this to law enforcement – there are no effective reporting mechanisms, let alone the police resource to take action. ISPs already participate in a great many law enforcement and education groups but the time has come to move from mere liaison and consultation to active co-operation and partnership. While legitimate ISPs shoulder both regulatory and voluntary burdens, they have a right to expect that it will be made much harder for criminal gangs to set up their own ISPs. Cleaning up the “who is” database should have much greater priority. Affilias, which registers the .info domain names, has joined the Internet Watch Foundation and introduced tight conditions of service. The IWF now expects to see those deregistered by Allifias rapidly re-register with less responsible registrars around the world. Tackling this problem is non-trivial. Nominet, for example handles over 7 million registrations a year.

The Internet Watch Foundation monitors trends and patterns around the world and the slow pace at which law enforcement reacts is a major problem. IWF operates one of 33 hotlines around the world sharing information but the websites commonly move on before law enforcement catches up. The UK achievement is impressive but the global achievement is not. One website has now been on the move around the world for a decade. There is a need for the national forces in the Global Virtual Task Force to share out the problem, allocating such sites to specific forces to take the lead in working internationally with industry and others to track these over time and home-in on the organisers.

A bigger problem than the naivety of end users is that of the police, They waste time and money because they do not know the right questions to ask when contacting ISPs and Telcos for assistance, including with regard to making sense of all the communications and other data that is now being retained. There is a need to ensure that all police receive relevant training and updating because most crime, not just fraud, now involves electronic communications and evidence. The formation of the PCEU should provide a focus for this but there is a need for people continuity to build up the quality and quantity of expertise.

We need to ensure that additional resources are directed to where they will have most effect, for example funding more SPOC (single point of contact liaison) officers, to enable enquiries from front-line investigators to be handled much faster than at present. Additional technical training, while useful, might not be as important as addressing the very basics of effective communication and partnership working.

There was a general view that most current legislation is fit for purpose, albeit some of it still needs testing in court. Only if it then fails should it be changed.

Many past initiatives to improve co-operation between industry and law enforcement, including those of the Internet Crime Forum, ran out of steam because of the lack of continuity of staffing and engagement on the part of government and law enforcement. While industry expertise is crucial to good design and security, Chief Executives look to government to make a commitment to supporting an initiative.

Much of the advice on offer is not conveyed to those who need it, such as victims, or is unrealistic or even illegal. For example those running businesses over Facebook or e-Bay may be advised to withhold their physical address: “lest thieves come round and steal their stock”. This is illegal under the e-Commerce directive, It was suggested they be advised to give the address of their accountant or bank manager instead!

With the understandable focus on child protection and fraud we must not forget the other harms being caused, such as the websites that encourage suicide, including among young people and even children.

The rights-holders whose software, videos or music are pirated over the network are amongst the biggest victims of e-crime and can bring much to any partnership, including their investigation resources and experience of running education programmes. They like to support law enforcement and most would rather also support education programmes than seek to criminalize a whole generation. It was suggested that one way to greatly improve co-operation was to accept that young people now see music on the Internet as the advertising to attract them to pop concerts: something to swap, not to pay for.

This was only one of a number of difficult questions, such as whether to give priority to training or to finding solutions to immediate problems, let alone freedom of speech versus child protection.

New technology, from the printing press to the telephone, has often given rise to moral panic. Who decides what is harmful? Meanwhile "mere conduit" protection gets in the way of "best efforts" partnership. Heavy-handed management of risk removes opportunities for children, (raised in captivity by parents too frightened to let them go out to play), to learn how to explore the on-line world safely. We want the Internet to be a seamless part of life but we must remember all those "middle aged children" haunting Second Life. Meanwhile we waste time on supposed panaceas: age verification can be improved but will still be circumvented by both adults and children.

It is when questions are difficult that partnership comes into its own. Partnerships are about creating a safer environment not chasing criminals. That is the job of the police. We are looking at a partnership of partnerships that cross boundaries, local, regional and national..

- What are the perceived problems?
- What actions will cut those problems?
- What is the cost of action?
- Who will pay

(usually different to who will benefit, hence the game of pass the parcel across government)

BUT also

- What is the cost of inaction?

and

- How do we ensure a cross-cutting approach that will engage the necessary players as the environment changes?

The Internet community has a number of models for global partnerships with a specific focus, such as spamhaus but the key to success is to have a strategic approach with the comprehensive engagement of business – especially companies who wish to see their customers able to engage with them confidently and safely on-line.

That means finding those who will take a lead in moving from reacting to initiatives and consultations to pro-active partnership and co-operation.