E-Crime Reduction Partnership

Good morning.

===================================
The E-Crime Reduction Partnership
- Current initiatives
- Objectives
- Progress
- Working Groups
- Business Case for Participation

“Why do the Criminals find it so much easier to co-operate”
Philip Virgo, The Information Society Alliance, EURIM
===================================

My objective is to give a progress report on the formation of the e-Crime Reduction Partnership and explain why participation should form part of your organisation’s on-line marketing strategy and not just the security strategy you have not got.

I have been piggy-in-the-middle between the IT industry and its victims, also called users, for over thirty years. In 1997 I moved from the dark side, my last post with an IT suppliers, and joined the strategic planning team for a multinational whose business was critically dependent on its brand image and knowledge base. That change also meant that I became trusted by politicians and was invited to work on national policy studies. Five years later I was head-hunted by the Director of the National Computing Centre to try to represent the user voice in the corridors of power – against the cacophony of supplier interests.

Today, in trying to make a reality of e-Crime Reduction Partnership that was announced in the Digital Britain Report, I find myself piggy-in the middle again.

This time between the IT Security industry and its victims. Those victims include the customers it frightens to death and the shareholders whose profits it fails to protect. Unfortunately the victims do not include the e-criminals – crying all the way to their money launderer. Meanwhile the evidence of reported losses appears to show that the e-security industry costs business rather more than the e-criminals. The real cost is lost business.

Now I will turn to last slide. I will go through the current initiatives, objectives and progress to date but – first - what is the business case?

===================================
The Business Case for Participation
- More customers transacting regularly on-line
- More profitable on-line operations
- Lower cost (including security) on-line operations
- Fewer attacks on you and your customers
- More sleep at night
=====================================

The objective of a physical e-Crime Reduction Partnership is usually to get more consumer spending more money in a town centre, more businesses making more money on a trading estate and more residents willing to pay higher house-prices and rents because they feel the area is safe. Spending more on CCTV Cameras, Locks and Bars inspires fear rather than confidence. Finding other ways of causing criminals to move elsewhere or find an easier ways of making money is more effective.

The objective of the e-Crime reduction partnership is similar.

It is to get more customers transacting regularly on-line because they feel safe and confident. It is not to frighten them into buying more scareware or into visiting only the websites of those market leaders who have been able to conceal their insecurity.

That does not mean more awareness campaigns. Your customers are confused and frightened enough already. It means fewer, more effective awareness campaigns, with many more participants, common messages, realistic advice that works, sources of support and redress that help, the feeling among customers that if they report problems some-one might take action, plus that warm glow of ***revenge*** when hear feel that ***their*** report to abuse@yourbusiness.co.uk might help convict a fraudster or pederast, or at the very least put a criminal registrar supplying domain names to spammers out of business.

I am use the term “criminal registrar” in much the same way as I might use the term “criminal lawyer”, one whose business may be legitimate but depends largely on providing services to criminals

We see hear a lot about the cost of e-crime. In fact the reported losses are piddling compared to what is spent on security, let alone what is written off as bad debts. The biggest cost is the lost business from those who did not transact with ***you*** because

- they got lost, fed-up or timed out in the entrails of your on-line security system,
- they got confused by all the security do’s and don’ts and decided it was safer not to
- they took the advice on strong passwords seriously and cannot remember what it was
- they only transact with those they trust, like Amazon,  John Lewis or Tesco .

Over half the UK population may have bought on-line “more than never”, but less than one in eight does so regularly – counting “more than once a month on average” as regular. Less than a quarter of those who advertise online are willing to transact on-line. Small firms especially fear that the cost of fraud is greater than the benefit from transacting on-line.

The equation is different for large organisations who also stand to gain more from getting more of their customers, to do more of their transactions on-line. The points of leverage for achieving that leap in confidence include co-operation to

- improve victim support,
- remove common points of vulnerability and also
- remove some the forty or so loose confederations of predators said to account for over half of all on-line crime and malpractice worldwide.

Those who work together to remove common vulnerabilities, to improve victim support and to remove and deter predators by funding and working with specialist police units, will get more value from the spend on awareness programmes because these can now be seen to linked to active co-operation to remove the causes of fear. They will also improve profitability and cut cost more than from merely spending more on security.

====================================

Current Initiatives

- Get Safe On-line
- Child Exploitation and On-line Protection Centre
- Police Central e-Crime Unit
- SOCA e-Crime
- National Fraud Authority
- Office of Cyber-Security
- ACPO e-Crime Strategy
- e-Crime Reduction Partnership

==================================

The announcement of the e-Crime Reduction Partnership in the Digital Britain Report described it as a tripartite co-operation of Government, Industry and Law Enforcement chaired by the Rt Hon Alun Michael MP.

Alun is a Director of EURIM and chairs its e-Crime Group. He was the Home Office Minister who drove the legislation to create Crime Reduction Partnerships. He knows what he wants. Many of you will have heard him describe the approach. I will not repeat it.

Instead I will describe the role of the e-Crime Group in creating the Partnership and invite you to join us in helping do so. I used to describe the role as that of midwife, but was told that midwives rarely deliver their own off-spring and I would frighten the professionals, nearly all of whom are men, with images of pain, blood and mess. Better to use the analogy of building and launching the first stage of a rocket to put a satellite into orbit.

Either way, our task includes supporting the launch by organising groups that provide a common industry front-end across the existing initiatives, organising pilot projects to demonstrate that co-operation produces results and reducing the cost of co-ordination.

For example, most of the groups on this slide support awareness programmes and there are many more, from the amateur or even fraudulent upwards. Meanwhile Get Safe Online has the support of Government, of major players like Microsoft, Google and e-Bay and of the two dozen or so trade associations and professional bodies that have come together in the Information Security Awareness Forum. However we still have organisations planning new awareness campaigns instead of building on what already exists. The main reason is that the Get Safe On-line delivery team are too busy delivering results on a very limited budget to be able to attend meetings to brief potential supporters and participants. And few potential supporters expect to be asked to make a financial contribution towards the cost of recruitment and co-ordination.

We aim to address that problem by organising briefing meetings and material which position Get Safe On-line alongside the other awareness campaigns supported by, for example, CEOP and the National Fraud Authority or the various anti-piracy groups and spell out the costs and benefits of participation.

There is a similar situation with those wanting to support, education and awareness programmes for children – complicated by the need for CRB checks on those volunteering.

None of the organisations on this slide has resource to on industry liaison, let alone agreeing a co-ordinated approach to recruiting support and explaining to potential supporters their different objectives and how they fit together and who to work with on what.

===================================

Objectives

- Build/preserve Confidence in the On-line World
- Reduce the fear of e-Crime
- Address the concerns of the User communities
- Facilitate co-operation across boundaries
- Make the UK a natural centre for Global e-Policing

====================================

Working across organisational boundaries to produce agreed ways forward is what EURIM does. It does not itself aim to do anything more. We are not bidding to run anything, other than activities which bring players together to organise co-operation that they will themselves then drive forward, via whatever channel they agree.

With regard to the partnership our objective is to focus on identifying what the concerns of the user communities and who is willing to contribute what towards addressing those concerns and enticing them back on-line, to be sold to and serviced at lower cost.

The fnal point on this slide is less ambitious than it seems. Most of the world's physical trade, whether by sea or air, is organised by contract authentication and freight-forwarding operations based in London. Most of the worlds commercial disputes resolution, alias policing, operations are based in London. That gives the potential for a similar position in the on-line world - even if the server farms are to be in the Rockies.

That has massive spin-offs for improving the quality on on-line policing in the UK.

====================================

Progress:
- November 30th - planning meeting
- January 22nd – academic review of knowledge
- January 26th – working group meetings start
- March 3rd – Ministerial/CEO engagement meeting
- Late March – industry commitment meeting
- April onwards – pilot projects come on-line
- Q3 – scoping exercise reports

“Bandwagon not rocket”

====================================

At the end of November we had a round table planning meeting to identify who was willing to help work on what. We found clear support projects in a number of areas but also a common concern that we had no real idea of the scale and nature of the issues we were trying to address. There was a major need for the “audit of reality” that has been the common start point for all successful e-Crime reduction partnerships in the physical world.

That audit of reality is what I refer to on this slide as a scoping exercise. It will be easy of cheap. That which lead to the creation of the National Fraud Authority cost £250,000 but secured £25 million of government funding and rather more from industry for the initiatives that will inter-work with it.

On 22nd January there was an academic round table to look at the current state of knowledge and the possible ways of mapping reality with regard to eCrime. That meeting confirmed the need for a more pragmatic approach based on the concerns of the target audiences rather than theoretical definitions. It also confirmed that the scoping exercise must address the concerns of those who control budgets and decisions and command credibility with them.

On the 26th of January we had the first of the meetings to plan interim projects: those activities worth progressing even without understanding the full scale and nature of the problems to be addressed.

Stephen Timms is Financial Secretary to the Treasury, as well as Minister for Digital Britain. He is one of those who needs to see the full business case and has agreed to himself chair the planned meeting of Chief Executives to get top level engagement from across Government and Business. There will then be a commitment meeting, with a rather larger invitation list. That “commitment” is to the scoping exercise and to act on what is reveals.

Will it, for example, produce evidence that would persuade HM Treasury that a hundred million or two towards on-line policing would cut a billion or two from the cost of tax and benefit fraud and generate a billion or two of taxable profit in the private sector. That scoping exercise is likely to take at least six months - hence the Quarter 3 on this slide.

In the mean time we hope that the more modest interim projects will generate confidence that co-operation produces results and make it easier to scale up rapidly to implement the recommendations from the scoping exercise.

======================================

Working Groups
- Awareness
- Small Firms
- Skills
- Forensics
- Intelligence sharing
- First point of contact
- Security by Design

=====================================

So where are we with the interim projects.

We have already had one meeting to look at bringing together the various awareness exercises, leveraging that which is done by large organisations to train their own staff as well as that being done by vendors. The next step is to have a larger meeting to invite potential business and commercial players to help lead the exercise and not just participate.

A lot is said about the needs of small firms. Usually by those who have never run one, other than in the sense of being a self employed IT or security contractor working for large firms. This group is building on the work done by those who support small firms with mainstream crime prevention advice, drawing in the small firms associations.

e-skills uk has funding from HMG to create an on-line National Academy for IT skills. The professional bodies, BCS, ISACA, ISC2, ISSA and so on have agreed to work with some of the main training providers and recruitment agencies to bring together material on current career development and accreditations and the relevant qualifications, courses and materials. We have also begun recruitment a cadre of employers to ensure that what is planned does indeed reflect their needs.

There are major issues to do with digital forensics, from training more people to better prioritise and handle current backlogs to producing the tools necessary for mobile and network communications and content. There is the potential to bring the necessary players together to address these – but this will require crossing traditional boundaries in new ways. The next meeting to explore how to achieve this is in about a fortnight.

Intelligence sharing is even more problematic because there are good reasons why some of the barriers exist. But not others. Thre is also a need to work across rings, as well as hierarchies, of trust

First points of contact: we have a jungle of would-be single points of contact. The issue is to network these so that no first point of contact is wrong. Who-ever you go to should be able to pass you to the right square. This group is particularly interesting because of the divisions between those who fear being deluged with problems that they cannot handle and those who see this as an opportunity to restoring consumer confidence by using automated tools to handle most problems and support human response to the exceptions. Meanwhile there are those who wish to have rapid collated data in order to prioritise operational responses and those who want historic data to justify budget bids.

Finally, Security by Design or default, as opposed to security by afterthought or accident, is central to most crime reduction programmes. A separate group is currently reviewing a report that makes recommendations that have widespread support. The issue will, however, be to turn those recommendations into action.

There are other groups but I am running out of time.

=====================================
The Business Case for Participation
- More customers transacting regularly on-line
- More profitable on-line operations
- Lower cost (including security) on-line operations
- Fewer attacks on you and your customers
- More sleep at night

=====================================

The objective is not to produce recommendations that impress security experts or get them more business. It is to get more customers transacting regularly on-line so that businesses have more profitable on-line operations.

That may well entail diverting some of security and marketing budgets to support improved co-operation with law enforcement and your partners and even your competitors to co-operate in deterring and taking out predators.

I will be staying for lunch and would be please to answer questions then or by e-mail if we run out time now.

My core objective today is, however, to ask you to email me with offers of assistance – saying what you are willing and able to contribute in order to achieve what.

This is a partnership not a project.

Thank you for listening.