

## **Technical Appendix to Annex 2: From Awareness to Action? On-Crime Prevention Programmes**

### **1 Background**

Until recently most on-line service providers were focussed on providing low cost, user-friendly access. E-crime prevention was seen as little more than encouraging users to buy and use anti-virus filters and firewalls. Law enforcement and government therefore gave it a similarly low priority. Financial services have given it rather higher priority, but are focussed on preventing costs and losses to themselves and their customers. And most e-crime by reported value, if not by volume, harm or distress, involves insiders, including to copy files of customer, client, patient or supplier details and/or to help bypass security controls.

In February 2004 "Protecting the Vulnerable" [www.eurim.org.uk/activities/ecrime/sme.pdf](http://www.eurim.org.uk/activities/ecrime/sme.pdf), published as part of the joint EURIM-IPPR study into "Partnership Policing for the Information Society", identified small firms seeking to do business on-line as a major point of vulnerability in business supply chains. It called for an awareness campaign and the provision of realistic advice, guidance, support and training. The next paper in that study, on Skills issues [www.eurim.org.uk/activities/ecrime/skills.pdf](http://www.eurim.org.uk/activities/ecrime/skills.pdf), called for government and industry to co-operate in organising similar programmes for wider audiences. We have since had a number of awareness campaigns, some very well publicised, but less action on support and training and the House of Lords report on Personal Internet Safety, [www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf](http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf), endorsed the EURIM message that "raising awareness of risks without developing the knowledge and skills to manage such risks could undermine confidence in the Internet".

### **2 The Threads of Crime Prevention**

Crime prevention programmes tend to have five main threads:

- promoting awareness of the risks and need to take action;
- support programmes, including to install and inspect/maintain security products and services;
- advice on risk management/avoidance, given the need to live/work/play in a given environment;
- education and training: from personal risk avoidance through crime prevention and security staff to those in a position to "design out" product, service and environmental vulnerabilities;
- risk reduction. to re-engineer the environment to make criminal behaviour less attractive.

#### **2.1 Awareness**

The National Cyber Security Alliance organises the US Stay Safe On-Line [www.staysafeonline.org](http://www.staysafeonline.org) website and campaigns which bring together the US Department of Homeland Security, Federal Trade Commission, and many private-sector corporations and organizations to promote awareness and provide tools and resources to empower home users, small businesses, and schools, colleges, and universities.

The "Be Safe On Line" website [www.besafeonline.org](http://www.besafeonline.org) was created as part of the Safer Use of Internet Services (SUSI) an Internet safety awareness project supported by the European Union Safer Internet Action plan [http://europa.eu.int/information\\_society/programmes/iap/index\\_en.htm](http://europa.eu.int/information_society/programmes/iap/index_en.htm) The UK partners were Learning and Teaching Scotland and the Scottish Parent Teacher Council

Get Safe Online, [www.getsafeonline.org](http://www.getsafeonline.org) is the closest thing in the UK to "a comprehensive unified source of information on online safety and security" (House of Lords). It is sponsored jointly by Cabinet Office (CSIA), DTI (now DBERR), Home Office, CPNI, Cable & Wireless, eBay, HSBC, Microsoft, SOCA and Symantec. It links to other sites, including IT Safe [www.itsafe.gov.uk](http://www.itsafe.gov.uk), for alerts on vulnerabilities, Bank Safe Online [www.banksafeonline.org.uk](http://www.banksafeonline.org.uk), Card Watch [www.cardwatch.org.uk](http://www.cardwatch.org.uk) and the Home Office site dedicated to identity theft issues [www.identitytheft.org.uk](http://www.identitytheft.org.uk). Most awareness sites also provide crime prevention advice: e.g. The "Personal Security Plan" or the "Spot and Stop Card Fraud retailer training pack", available for download from the Card Watch site.

Childnet International [www.childnet-int.org](http://www.childnet-int.org) has a remit to make the Internet “a great and safe place for children” and its programmes are widely supported by industry, including with volunteers (vetted as necessary) to work with and inside schools. The Department for Children, Schools and Families (DCSF) <http://publications.teachernet.gov.uk/default.aspx?PageFunction=productdetails&PageMode=publications&ProductId=DCSF-00685-2007&> has published, in conjunction with Childnet, guidance for schools on preventing and responding to cyberbullying. The Child Exploitation and On-Line Protection Centre [www.ceop.gov.uk](http://www.ceop.gov.uk) has integrated services covering advice, guidance and reporting. Its awareness campaign in October 2006 was widely covered in the press and national media. The Internet Watch Foundation [www.iwf.org.uk](http://www.iwf.org.uk) runs a hotline for reporting potentially illegal child sexual abuse content hosted anywhere in the world and criminally obscene and incitement to race hatred content hosted in the UK. The IWF also provides a universal ‘notice and takedown’ service to any British service provider hosting potentially illegal content within their remit.

Awareness is now said to be less of a problem than “conflicting and impractical advice and guidance” on how to react. “The typical user ... buys a computer as a consumer electronic appliance, plugs it in and uses it; attempts to turn up the “security level” of his browser will cause some web sites not to work: he has no way of telling good security software from bad; and many of the problems are completely outside the control of even technically sophisticated users” (FIPR evidence to House of Lords).

## 2.2 Support for consumers and small firms

Mainstream crime prevention programmes commonly include routines whereby crime prevention officers and other security advisors will put householders and small firms in touch with local security firms who will check their premises and install locks and alarms. Most e-crime prevention advice refers to fitting anti-virus protection and firewalls as being the electronic equivalent of fitting locks and alarms. But the current provision of installation and maintenance support is akin to that when the NSCIA (subsequently part of NACOSS and now embedded within the UK National Security Inspectorate [www.nsi.org.uk](http://www.nsi.org.uk)) was formed in 1971 “to deal with the problem of poor quality equipment and *cowboys* within the intruder alarm market.”.

The NSI does not cover electronic security systems (other than fire and burglar alarms etc.) and the professional bodies and trade associations for the ICT industries were united in their opposition to the Security Industry Authority covering those providing electronic security advice, guidance and support - although current legislation may give it the power to do so. Meanwhile the main US suppliers of personal computers sponsored the creation of a new qualification, security +, by the Computing Technology Industry Association [www.comptia.org](http://www.comptia.org) (which they had created in 1983 to improve the skills of the dealer support staff whose competence they saw as critical to their sales, marketing and customer satisfaction).

The House of Lords called for the proposals for a BSI kitemark for content filtering (supported by the Home Office and Ofcom) for child protection purposes to be extended to cover security software (because of the difficulty of understanding what current products and services do or do not do) and social networking sites (because of the perceived risks). They also called for an ongoing review of “possible areas where codes of best practice, backed up by kite marks, might be appropriate.” Others have also called for action to:

- provide users with easy ways of establishing how secure their systems are, the threats they face and the balance of risk, facilities, speed and ease-of-use appropriate for business, learning and leisure use;
- develop schemes (from plain English consumer information packs through to specifications for technicians and professionals) to show what security facilities are built into which products and services and to which security profiles/standards they conform;
- pre-install security facilities, configured to the security levels required by the average user (i.e. average for the market into which the systems is being sold) with clear information on what this means and how to customise facilities, performance and security according to the planned usage.

ID theft and impersonation are major concerns. Experian [www.experian.co.uk/creditreport/](http://www.experian.co.uk/creditreport/) and Equifax [www.econsumer.equifax.co.uk/consumer/uk/](http://www.econsumer.equifax.co.uk/consumer/uk/) both offer chargeable services to alert consumers when anyone seeks to take out credit in their name. They are also in discussions with the National Consumer Council

regarding a collective “credit repair” service, possibly along the lines of that available in the US for the customers of the main financial services players.

The Metropolitan Police Service, as lead e-crime force, is in the process of creating the Police Central e-crime Unit (PCeU) with a view to mainstreaming e-crime issues into everyday policing. Meanwhile, it has delivered e-crime awareness training to the 140 MPS Crime Prevention Officers with a view to the messages being delivered to individuals and SME's across London. Negotiations are underway to extend e-crime awareness training to Safer Neighbourhood Teams in all 633 Wards across London. The SNTs have a key role in delivering a partnership crime prevention response to the community, including via all schools and education facilities. The MPS also maintains the Fraud Alert website [www.fraud.alert@met.police.uk](http://www.fraud.alert@met.police.uk) which offers e-crime awareness advice to both individuals and business. There are ongoing negotiations to formalise e-crime prevention advice standards and intelligence feeds with the new National Fraud Reporting Centre, e-crime Wales, CPNI and others. The MPS also has responsibility for e-crime prevention/threat assessments re the Olympics and, as part of operation Sterling, delivers e-crime prevention advice through 12 industry partnership development forums (hotel groups, construction, retail, etc.).

Yorkshire Forward [www.yorkshire-forward.com](http://www.yorkshire-forward.com) and its four regional police forces developed [www.yorkshire-safe.org](http://www.yorkshire-safe.org), administered by Sheffield Hallam University. The website is still evolving but is a portal to enable ICT basic adopters in SMEs to check their e-security vulnerabilities and then undertake some basic training. Updates to provide advice on wireless network security will follow soon. Yorkshire Forward also funds, with EU Objective 1 support, a business crime reduction centre [www.bcrc-uk.org](http://www.bcrc-uk.org) to promote e-business by ensuring SMEs have adequate security both physical and virtual. A small back office team, including a crime analyst is based in Sheffield supporting field officers who are co-located with the local Chambers of Commerce to give a business focus to their activity. This allows access to the Chambers' business networks also helping the co-ordination of other ICT activities, including those funded by Yorkshire Forward (E-business Unlimited etc). Regional roll-out is due to start next year and may be linked to WARP and e-business continuity issues (including those arising from the recent flooding).

Advantage West Midlands [www.advantagewm.co.uk](http://www.advantagewm.co.uk), West Midland Police [www.west-midlands.police.uk](http://www.west-midlands.police.uk) and the Cybersecurity Knowledge Transfer Network [www.ktn.qinetiq-tim.net](http://www.ktn.qinetiq-tim.net) are supporting a “National E-Crime Prevention Centre” [www.necpc.org.uk](http://www.necpc.org.uk) based on the University of Wolverhampton. This Centre will be a hub for research and training rather than an operational centre, but will also host crime prevention support services for small firms and regional WARPs (Warning and Access Reporting Points) for Local Government and Healthcare.

The national register for Warning, Advice and Reporting Points [www.warp.gov.uk](http://www.warp.gov.uk) currently lists four public sector WARPs, seven for local government, two for business, two for the voluntary sector and one international. Some are specific to a group (e.g. RAYWARP for radio amateurs) or supplier (e.g. BTRWARP for customers of BT Retail), others are geographic (e.g. SKWARP for Local Authority Partners in Kent) or national (e.g. IG WARP for the National Health Service).

### **2.3 Support to Schools and Colleges**

The British Educational Communications and Technology Agency [www.becta.org.uk](http://www.becta.org.uk) has a remit to provide advice and guidance to schools, but only when they request it. The Regional Broadband Consortia organise on-line services for schools (see [www.ja.net/community/schools/england/index.html](http://www.ja.net/community/schools/england/index.html) for a list) and can (and most do) require their suppliers to provide guidance to the schools they serve, whether requested or not.

UKERNA runs the UK's Joint Academic Network [www.ja.net](http://www.ja.net). Its security team provide advice and guidance on information security and crime prevention to those connected to the network. Most Universities provide guidance to those who use their campus networks but the actual support to individual departments, let alone students, varies widely as do their approaches to security. Federal structures, to preserve the integrity of the network and prevent cross-infection while allowing freedom of action, are common.

## 2.4 Support to large organisations

There is a billion pound industry selling “security solutions” to those who can afford to pay for customised services. A variety of professional bodies, trade associations and security “clubs” are also competing to provide collective advice and head off the risk of intervention by bodies from outside their world: from the Financial Services Authority and Security Industry Authority to the Home Office or Ofcom.

There are also groups seeking to bring together specific industry sectors or communities of large users to take action against common problems, including by presenting their technology suppliers with common requirements for security products and services or by developing common processes for dealing with government, law enforcement and others.

Thus the main telecoms players support TUFF [www.tuff.co.uk](http://www.tuff.co.uk) the Telecoms UK Fraud Forum and MICAF ([www.micaf.co.uk](http://www.micaf.co.uk) the Mobile Industry Crime Action Forum). These share offices and staff, have overlapping memberships and address issues of investigation and detection as well as of prevention through sharing of best practice and training.

CIFAS (the Credit Industry Fraud Avoidance Service) [www.cifas.org.uk](http://www.cifas.org.uk) serves a rather larger community, albeit with a more limited remit. It describes itself as “the UK's Fraud Prevention Service with 260 Members spread across banking, credit cards, asset finance, retail credit, mail order, insurance, savings and investments, telecommunications, factoring, and share dealing.” Its members “share information about identified frauds in the fight to prevent further fraud.” (i.e. it maintains lists of known or suspected fraudsters so that their subsequent attempts to defraud its members can be more rapidly identified).

The APACS [www.apacs.org.uk](http://www.apacs.org.uk) Industry Hot Card File (IHCF) enables its 80,000 retailer subscribers to check transactions against lost or stolen cards and is increasingly being used by e-commerce retailers (not just in the UK) for card checking before the dispatch of goods. It is credited with having prevented over 750,000 cases of attempted fraud over the past two years and is, for example, now being used successfully at motorway tollbooths in France to combat the use of stolen UK credit cards.

The Jericho Forum [www.opengroup.org/jericho](http://www.opengroup.org/jericho) brings together many of the world's largest users of security products and services to “define ways to deliver effective IT security solutions that will match the increasing business demands for secure IT operations in our open, Internet-driven, globally networked world”.

Large scale and high value ID fraud commonly involves the theft of information by insiders, including in the public sector. On 27<sup>th</sup> June 2007 the UK Government launched a new “National Information Assurance Strategy for the UK” [www.cabinetoffice.gov.uk/csia/documents/ia\\_strategy/ia\\_strategy.pdf](http://www.cabinetoffice.gov.uk/csia/documents/ia_strategy/ia_strategy.pdf) This is owned by “The Officials Committee on Security” (Chief Information Security Officers), the “Information Assurance Policy and Programme Board” and the CIO Council. It will be driven forward by CSIA, CESG and CPNI with industry collaboration via groups such as the Crypto Developments Forum and the Information Assurance Collaboration Group. The challenge is summarised by Independent Review of Government Information Assurance [www.cabinetoffice.gov.uk/csia/documents/ia\\_strategy/ia\\_review.pdf](http://www.cabinetoffice.gov.uk/csia/documents/ia_strategy/ia_review.pdf)

Unlike much of the public sector, the regulated financial services industries are already required to demonstrate that they have such policies in place as a condition of being allowed to do business. Moreover, those who participate in the main industry transaction and supply chains are usually contractually liable for any breach, under terms and conditions that tend to go well beyond those required by the relevant regulators.

## 3 Advice on Risk Management

Advice on avoiding unnecessary risks and recognising potentially dangerous situations is a common thread in crime prevention programmes. The most effective programmes put this into business context e.g. how to reduce the risk of shoplifting while having displays that will attract potential paying customers and entice them from browsing to into paying.

This area is not well covered with regard to e-crime prevention. There are tensions not only between “marketing” and “security” but also between those wishing to promote low cost, user-friendly services to young bargain hunters with short attention spans and those wishing to promote confidence in higher value transactions on the part of wealthier, older, more risk averse customers.

One manifestation is the clash between advice to ignore e-mails purporting to come from Banks, especially those warning of security breaches or offering security upgrades or new services, and the marketing exercises commissioned by Banks which often lead to outside agencies commissioning on-line surveys in their name, some-times linked to genuine offers.

The evidence by Linda Criddle to the House Of Lords (section 6.39 onwards) highlighted a similar clash between advice not to give out personal information and the regular encouragement to children and teenagers to give this out on social networking sites.

There is a need for much greater awareness among those wishing to deal with their customers/clients/voters on-line as to what is good practice on their part with regard to building customer expectations, as well as with regard to safeguarding the customer information data they have acquired. The Code of Practice [http://www.ico.gov.uk/upload/documents/library/data\\_protection/practical\\_application/ico\\_information\\_sharing\\_framework\\_draft\\_1008.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/ico_information_sharing_framework_draft_1008.pdf) on which the Information Commissioner has just consulted is relevant. So too is the Californian legislation regarding the reporting of data breaches and the extension that is about to come into force, [www.out-law.com/page-8476](http://www.out-law.com/page-8476), requiring the deletion of data that would enable card protection schemes to be bypassed.

#### **4 Education and Training**

Training in the installation of security products is rarely part of traditional crime protection programmes. The expectation is that locksmiths and security firms will do this. It does, however, form a major component of programmes to encourage safer Internet use. Given that barely 20% of Internet users have received any training (2007 Oxford Internet Institute Survey [www.oii.ox.ac.uk/microsites/oxis/](http://www.oii.ox.ac.uk/microsites/oxis/)) this is, perhaps, not surprising. But the implications are profound and the consequent need for action goes well beyond the awareness and self-protection skills needed by end-users

The accompanying paper on Cybercrime Awareness, Education and Skills [link].summarises current activities and responsibilities for identifying the knowledge needed and by whom. It also covers those for organising and delivering the education, training, assessment and accreditation programmes required.

#### **5 Risk Reduction**

Redesigning the environment to discourage criminal behaviour is a major part of traditional crime reduction programmes. The actions can be cheap and/or visible: e.g. redesigning lighting in a shopping mall or replacing glasses by plastic in city centre bars. They can be “invisible” but still relatively inexpensive: e.g. the raised “flowerbeds” or ornamental “benches” that will stop a 10 tonne truck at 40 mph (the NATO specification for defence against suicide bombers and equally effective against ram-raiders). Or they can be very expensive: e.g. demolishing a crime-ridden shopping mall or housing estate that won an architectural award for innovative design twenty years ago.

There is now a high level of awareness on the part of business, with surveys indicating that over 60% now have filters, firewalls etc. However the Oxford Internet Institute survey, the best indicator of current consumer behaviour, indicates that while most end-users are aware of the problems, less than half have done anything about them. Many of those in the ICT world, including enthusiastic end-users, appear to still be at the stage of admiring novelty and innovation, rather than thinking through the consequences.

But it may be that much can be done without trying to “redesign the Internet”. The House of Lords report contains much food for thought on how to achieve this and the current state of debate and resultant initiatives are considered in the accompanying paper on Designing Out Opportunities for E-Crime. [www.eurim.org.uk/activities/ecrime/PIC07\\_techapp\\_designingout.pdf](http://www.eurim.org.uk/activities/ecrime/PIC07_techapp_designingout.pdf)