UK Information Security Awareness Forum Meeting - 17th September 2012

Location: The Information Technologist Hall, 39a Bartholomew Close, London, EC1A 7JN

Time: 14:00 – 17:00

Purpose: Review of UK Information Security Awareness Programmes, including plans for Get Safe On-line

Present:
Liz Bacon (BCS, CPHC)
Basil Cousins (Open Forum Europe, WCIT, Ethical & Spiritual Committee)
Emmanuelle Filsjean (ValidSoft)
David King (ISSA)
Anu Khurmi (Cyber Champions)
Carsten Maple (CPHC)
Alexandra Moore (National Fraud Authority)
Tony Neate (Get Safe Online)
Carl Ricketts (Citibank)
Sarbjit Sembhi (ISACA)
Howard Skidmore (WCIT)
Graeme Smith (WCIT)
Martin Smith (The Security Company)
Lyndsay Turley (ISC2)
James Willison (ASIS)
Edward Wolton (WCIT)
Eva Zuckschwerdt (National Archives)
Kabir Babber (LSE Cyber Champion)

Apologies:
Louise Bennett (BCS)
Hilary Coote (Detica)
Andrew Cunnington (ISSA)
Roger Ellis (ISSA)
Tim Holman (ISSA)
Roy Isbell (DeMontfort University)
Kevin Jones (CPHC)
Roger Marshall (SOCITM)
Dan Mount (EURIM)
John Palfreyman (IBM UK)
Chris Rees (WCIT)
David Rennie (Cabinet Office)
John Riley (WCIT)
Andrew Yeomans (ISSA)

Time	Speaker
14:00	1.Welcome and introductions • David King • Philip Virgo
14:20	2.Review of awareness programmes targeted at UK audiences • Open forum
14:50	3.Presentation of research findings on changing target audience behaviours • Carsten Maple
15.45	4.Presentation on Get Safe On-line 2012 campaign • Tony Neate
16.15	5.Presentation on National Fraud Authority plans • Alex Moore
16.45	6.Discussion and general review of ISAF forward plans • Open forum

1. Welcome and Introductions

- ISAF was created at the instigation of the ISSA to co-ordinate the activities of over 20 professional bodies and trade associations. Its achievements include the production and distribution of a widely used set of Directors Guides and an exercise on the need for convergence between electronic and physical security.

- At a review meeting on June 14th 2012 those present agreed to explore a more commercial focus, inviting corporate participation via its member organisations with a focus on sign-posting, information exchange and the cross-fertilisation of ideas rather than organising projects.

- They agreed to meet in three months time after the Olympics, to review the future on the ISAF in the light of reports on the current state of play on awareness programmes and on research into behaviour change. This is that meeting and will also be asked to consider restructuring the ISAF as part of an industry-led quarterly review mechanism with ministers and their relevant officials from Home Office, Cabinet Office, BIS, MoD etc. invited as guests. Thus James Brokenshire MP and Ian Caplan might be invited from Home Office.

- Each quarterly review meeting would have a couple of major items for discussion but the prime aim would be to help the industry participants review value for money in deciding where and how they put their own efforts, given the competing initiatives and demands on the time and resources they have available.

2. Review of the information security awareness programmes targeted at UK audiences

- The tabled draft included global programmes with a UK footprint, and UK-based programmes which aim to reassure global audiences that the UK is a safe location for doing on-line business

- Participants were asked to identify obvious errors and omission and suggest where they should be included. One was the SASIG which it was agreed should be included under professional awareness, because it membership was those running staff awareness campaigns within their own organisations.

- **ACTION Alexandra Moore to provide the Fighting Fraud Together grid of communications awareness activities to enable the table to be updated [and has since done so – sent separately as an excel file].**

- We should reference the relevant cyber security guidance provided by GCHQ and CPNI in the sections on professional and executive awareness [done – see appendix]

- We should reference the material produced by the National Archive for non-technology aware public sector organisations: **ACTION - Ed Wolton and/or Eva Zuckschwerdt to provide the links**.

- We should discuss the means of progressing co-operation on the integration of physical and electronic security awareness programmes with the ASIS convergence sub-committee. We will need action plans to address the gaps, or at least identify the channels for doing so. It was suggested that ASIS (with their focus on business risk) should pick up on awareness issues from physical security side **ACTION James Willison to progress**. Open Forum Europe, which has a stream looking at Open Standards in ICT security might be asked to focus on end user device issues **ACTION Basil Cousins to see what might be practical**.

- Open standards are essential to effective integration and therefore need to be on the agenda. There was a short discussion on the different definitions of “open” (e.g. some US players consider proprietary standards as “open”). HMG aims to publish a policy document, including a definition of “open” before the end of the year.

- We should aim to work with GCHQ on cyber standards and build on their desire to remove complications and simplify because the current complexity increases risk.

- The mapping exercise must lead towards recommendations as to what to do regard to the gaps found. Market forces (e.g. industry taking informed decisions as to which programmes to support) may be a better way of reducing duplication of effort than attempts at collegiate decisions but we will need to propose ways of handling the gaps we identify. If we do not who else will. **ACTION discussion of possible proposals should be an item on the agenda of the next review meeting.**

3. Review of the state of research into target audiences and how to change their behaviour

- There is a large body of academic material and there are many researchers looking at the behavioural aspects of security and at training issues. We need to determine how we identify the target audiences and the material that is relevant. Consumers, Small Businesses and IT professionals are very different audiences. Each will also have sub-groups with different attitudes and patterns of behaviour, including towards risk, fraud and the internet.

- A particular need is to change the behaviour of systems designers and developers so that they produce applications which are secure by design and default. One global bank, tired of spending large sums on penetration testing to discover that new systems replicate old vulnerabilities, has produced its own mandatory training modules for in-house staff and for contractors. The need to assess the security of business partners inhibits co-operation and shared services. There is therefore a need for such approaches to be embedded in mainstream computing, communications and electronics degree courses.

- SANS www.sans.org were said to have looked at what works but how and why does it work? e.g. with regard to guidance for small firms

- **ACTION: We need to encourage the BCS and IET to review the security requirements for the courses they accredit. Liz Bacon (as chair of the BCS Academic Accreditation Committee) agreed to lead on this. Philip Virgo agreed to ask Hugh Boyes (IET lead on Cyber Security) where things had got to within IET after he raised it discussion at Greenwich on May 21st**

- We might recommend a top ten Information Security list for universities and higher education institutions to include in degrees, so that they can be accredited. If so, this should link to work currently underway by GCHQ. **ACTION Edward Wolton to suggest the necessary link.**

- Knowledge is the easy bit but behaviour is a function of attitude. The most important part is changing individual attitudes. The common trigger for behaviour change is crisis. How can we use the ***risk*** of crisis to encourage change without waiting for the crisis? The means of bringing about behaviour change is not yet included in academic foundation material on information security. There is a need/opportunity to address the gap. The example was given of the Verizon R&D operation where 10% of staff were anthropologists – ensuring the products were designed to meet the needs of human beings, testing they did so and also handling relationships between R&D and the rest of the organisation

- Should we (ISAF and/or CPHC) seek to create and maintain a grid of relevant research and training activities? We need to know who would value and use the results? We also need to know who would maintain it because we do not wish to merely add another to the many unmaintained maps.

- There is a widely perceived need to improve trust in the Financial Services industry and behaviour change is core to building trust.

- **ACTION: Alex Moore to provide links to the behaviour analysis research for the Fighting Fraud Together campaign, including that on SMEs published today (13 segments (7 consumers, 6 SMEs). Done.**
    - The report of the Consumer segmentation research is at www.homeoffice.gov.uk/publications/agencies-public-bodies/nfa/national-fraud-segmentation?view=Binary .
    - The report of the SME research is at www.homeoffice.gov.uk/publications/agencies-public-bodies/nfa/sme-fraud-segmentation
    - The reports categorise the audiences into segments, grouped according to their attitudes and behaviours towards risk, so that appropriate security measures can be identified ,ways to tackle that behaviour and implementation plans can be agreed and monitored, and success evaluated.

- **ACTION: Carsten Maple to initiate CPHC discussion on classifications to be used on the ISAF website and how the resultant taxonomy can help classify academic work on awareness and behavioural change**

4. Plans for the Get Safe On-line 2012 campaign and discussion of support from ISAF members

- The campaign runs from 22nd-26th October 2012, has a primary target of 14-16 year olds and is built around encouraging companies to support and collaborate in activities which promote cyber security awareness by encouraging the target audience to "click and tell": looking at the messages and telling friends and family their ideas on how to be secure.

- The support campaign includes celebrities giving their tips, the PR co-ordination of news stories to get prime time media cover, advertising and social media exercises and a programme of railway station and shopping centre promotions and school and university visits built around (but not confined to) a tour bus. Support materials include T-shirts, button badges, foam hands, posters, leaflets, pop-up stands etc

- A prime requirement is for "experts" to be available to answer questions at the events. All ISAF members will be asked to trawl their respective memberships accordingly. Some, like ISC2 and Cyber Champions have already started doing so and/or have agreed to help specific schools and other activities. Tony Neate will provide details on timings, addresses and the kinds of expertise and commitment sought.

- **ACTION: David King will e-mail the ISAF network after receiving the necessary information from GSOL**

- **ACTION: Philip Virgo will similarly e-mail the WCIT Security Panel and will also contact IT4Communities and those running the Journeyman programme with a view to requesting e-mails for volunteers.**

- It was agreed to recommend that organisations with their own staff and customer awareness campaigns be encouraged to use the opportunity to get publicity for what they are doing but such efforts should be notified in advance, given the danger of overloading the press with stories during the campaign week.

- There was caution over the idea of promoting a variation on "click and tell": encouraging organisations to have a click button on all web pages to take users to their routines for problem handling (e.g. from reporting possible abuse or impersonation to problems making transactions). This was because of the risk that such a button would be impersonated and thus become a point of vulnerability. The idea needs refining.

5. National Fraud Authority Plans

- NFA had looked at which groups of people were vulnerable to certain types of fraud and why. They were also evaluating the effectiveness of the material they had produced in the light of that segmentation: thus 66% of those who saw the targeted videos said they were more aware of how their personal information could be used

- The NFA is developing campaigns of activity targeted at 3 specific segments:
  - Consumer segments 2/2b: Often elderly and isolated, predominantly women who prefer face-to-face contact and are particularly vulnerable to bogus tradesmen and mass-marketing fraud
  - Consumer segments 4&6: Risk-taking (mainly male) investors who fall prey to investment scams such as boiler-room scams
  - SME Segment E: SMEs with turnover between £20-£40 million (i.e. large enough to attract a targeted scam but with security which has not kept pace with business growth), who are concerned about fraud and online crime and have taken some steps to protect themselves, but still fall victim

- The government's cyber security and awareness strategy aims to deliver measurable solutions to improve both the perception and reality of the UK as a safe place to do business online.

- By end of March the NFA will deliver a proposal to the government for which the core thread will be about improving online confidence and safety, supported by a programme of measurable, high-impact, high-visibility activities. It will include commitments of private sector co-funding (e.g. banks working together as an industry) and highlight the gaps in the current activity, where government intervention may be required to help protect those in society whose needs are not being addressed by others

- The activity proposals will also address why people are more open to risk-taking in the virtual environment, assess how confident and safe people are online and include proposal for a two-year tracking research study (starting in April 2013) to identify if/how people are indeed changing their behaviours – and therefore whether the activies are having the desired lasting impact on individuals' and SMEs' online safety behaviour,

- **ACTION: Alexandra Moore will use the next ISAF meeting to provide an update on the proposals and request feedback. This will be a main agenda item and will help determine the date of the meeting.**

- It is important to put awareness information into cultural contextual; segmenting social and religious groups and presenting material in the correct language needed to connect to such groups via the different channels available (e.g. community leaders, women's groups).

6. Open forum discussion and general review of ISAF forward plans

- Prior to the meeting, the intention was for ISAF to focus on information exchange between those running awareness and behaviour change programmes with quarterly meetings to review progress with invited audiences of potential participants and supporters. Those progress reviews would also feed into a cross-cutting industry group (organised by the Digital Policy Alliance and co-chaired by Stephen Mosley MP and John Palfreyman of IBM, which would look at cyber security issues as a whole from the perspective of those being called on to co-operate in their own and the public interest. The ISAF review meetings would, however, need to have added value for those taking time out from busy day jobs: public good and/or yet another networking forum was not enough.

- A progress report on the actions agreed above plus a wash-up on the Get Safe On-line and other campaigns planned this autumn and a presentation and feed-back session on the plans being made for next year will probably yield the necessary added value, provided is also helps deliver the opportunities for direct academic and commercial benefits that participants will need in order to justify their time in the face of current budget cuts.

- **ACTION all ISAF members to be asked if they are content with the change of focus and terms of reference to an information exchange and quarterly review operation which collates and cross fertilises the activities of its members and feeds the results into the Digital Policy Alliance e-Crime steering group and the ISSA advisory board, rather than trying to organise projects itself.**

7. Summary of Actions from the Meeting: “If we do not, who else will”

7.1 Review of Information Security Programmes

- Alexandra Moore to provide the Fighting Fraud Together grid of communications awareness activities to enable the table to be updated [and has since done so – sent separately as an excel file].

- Ed Wolton and/or Eva Zuckschwerdt to provide links to the material produced by the National Archive for non-technology aware public sector organisations.

- James Willison to progress co-operation on the integration of physical and electronic security awareness programmes with the ASIS convergence sub-committee.

- Basil Cousins to see what might be practical with regard to asking Open Forum Europe to focus on awareness issues with regard to standards and end user device issues.

- Dave King and Philip Virgo to include discussion of routines for handling identified gaps on the agenda of the next review meeting and call for proposals.

7.2 Review of the state of research into target audiences and how to change their behaviour

- Liz Bacon will lead on review of security requirements for BCS accredited courses.

- Philip Virgo to ask Hugh Boyes (IET lead on Cyber Security) regarding the position in IET[t]

- Edward Wolton will suggest links to the work being undertaken by GCHQ on accreditation

- Alex Moore to provide links to the behaviour analysis research for the Fighting Fraud Together campaign, including that on SMEs published today
  - The report of the Consumer segmentation research is at www.homeoffice.gov.uk/publications/agencies-public-bodies/nfa/national-fraud-segmentation?view=Binary .
  - The report of the SME research is at www.homeoffice.gov.uk/publications/agencies-public-bodies/nfa/sme-fraud-segmentation

- Carsten Maple to initiate CPHC discussion on classifications to be used on the ISAF website and how the resultant taxonomy can help classify academic work on awareness and behavioural change

7.3 Plans for the Get Safe On-line 2012 campaign and discussion of support from ISAF members

- David King will e-mail the ISAF network after receiving the necessary information from GSOL

- Philip Virgo will similarly e-mail the WCIT Security Panel and will also contact IT4Communities and those running the Journeyman programme with a view to requesting e-mails for volunteers.

7.3 National Fraud Authority Plans

- Alexandra Moore will use the next ISAF meeting to provide an update on the proposals and request feedback. This will be a main agenda item and will help determine the date of the meeting.

7.4 Open forum discussion and general review of ISAF forward plans

- ISAF members to be asked if they are content with the change of focus and terms of reference to an information exchange and quarterly review operation which collates the activities of its members and feeds into the Digital Policy Alliance e-Crime steering group and the ISSA advisory board, rather than trying to organise projects itself.

8. Date of next meeting

- Late November/early December to be determined by when the National Fraud Authority are ready to consult on their plans for 2013.

Appendix: “Map” of Awareness Sites, Campaigns and Organisations as amended after 17th September

1) Generic

Get Safe On-line www.getsafeonline.org Supported by UK Government as “flagship” awareness guidance website. Next national awareness week commences 22nd October

Safer Internet Centre http://www.saferinternet.org.uk/

Action Fraud, www.actionfraud.org.uk awareness, guidance and reporting mechanisms for scams, fraud and phishing. run by the National Fraud Authority

National ID Fraud Prevention Week (1-5 Oct) - 'Your information is valuable' PR campaign Partners: Fellowes (lead), Symantec, Equifax, NFA/AF, MPS

BBC Webwise www.bbc.co.uk/webwise/ : The BBC's guide to using the internet.

Information security Awareness Forum : www.theisaf.org co-ordinates awareness activities of over 20 UK trade associations and professional bodies.

Warning Advice and Reporting Points www.warp.gov.uk ; UK network of regional and sector consortia to exchange and distribute information on threats

Based outside the UK

Stay Safe On-line www.staysafeonline.org US exercise run by the National Cybersecurity Alliance. Next national awareness month, October 2012 (i.e. parallel with Get Safe Online.

Good to Know www.google.co.uk/goodtoknow/online-safety Google Online Safety campaign focussed on use of secure authentication processes for webmail.

Stay Smart On Line http://www.staysmartonline.gov.au/ Australian awareness programme

Internet Safety Project www.internetsafetyproject.org Sponsored by Verizon, Brigham Young University and Sorenson Foundation, global list of organisations and resources (last updated four months ago)

2) Children and Family

Thinkuknow www.thinkuknow.co.uk guidance and materials website organised by CEOP in association with Childline, Internet Watch Foundation, UKCCIS and Insafe.

Childnet International http://www.childnet.com runs a portfolio of sites including:

- UK Safer Internet Centre www.saferinternet.org.uk resource centre co-funded by EU, Internet Watch Foundation and SW Grid for learning. UK lead on annual ISOC “Safer Internet Day”
- Kidsmart http://www.kidsmart.org.uk/ help, advice and guidance materials
- Chat Danger www.chatdanger.com guidance on social networking behaviour
- Blog safety www.childnet.com/blogsafety/index.html guidance on blogging behaviour
- KnowITall www.childnet.com/kia/secondary/ guidance for teachers
- Digizen www.digizen.org guifance for children, parents and teachers on on-line conduct

Childline www.childline.org.uk help and advice – run by the NSPCC

Cybermentors: www.cybermentors.org.uk for bullying issues - run by beatbullying

Kidscape www.kidscape.org.uk/helpline/index.asp anti-bullying and abuse charity

Cyber Champions: http://www.cyberchampions.org/ employers providing young professionals as mentors to deliver workshops in schools within the national curriculum using CEOP approved material

Out Of Your Hands www.outofyourhands.com/ to educate young people aged 7 to 16 on the responsible way to own, operate and safeguard your mobile phone.

The Devil's in Your Details www.actionfraud.police.uk/thedevilsinyourdetails targeted at young adults (18 – 25) who are careless with their personal details and women (36 – 55) who lack awareness of the risks

Direct Gov http://www.direct.gov.uk/en/Parents/Yourchildshealthandsafety/Internetsafety/index.htm Internet Safety page of Direct Gov, contains cross links to Get Safe Online, Action Fraud, CEOP etc.

Wise Kids www.wisekids.org.uk/Kids_safe_search_engines.htm Search engines for Kids and Families produced by ICRA (the content rating agency). Does not include market leaders like Google or Bing

Safe http://www.safe.met.police.uk/internet_safety/get_the_facts.html Metropolitan Police website, similar cross links to those of Direct Gov.

Mumsnet www.mumsnet.com/internet-safety guidance and chat room for mothers on most topics but no links to other guidance sites.

UK Council for Child Internet Safety http://www.education.gov.uk/ukccis/about co-ordinates activities of over 180 members including major internet service suppliers and children's charities.

Child Exploitation Online Protection Centre, www.ceop.gov.uk for reporting grooming or other illegal behaviour:

Internet Watch Foundation (IWF), at www.iwf.org.uk for online child sexual abuse images, criminally obscene adult content as well as non-photographic child sexual abuse images

True Vision, at www.report-it.org.uk for content which incites hatred on the grounds of race, religion and sexual orientation

ParentPort at www.parentport.org.uk for content (broadcast, printed, games etc.) that may not be criminal but is unsuitable for children to see or hear

Youth 2 Youth: www.youth2youth.co.uk young persons helpline which offers confidential peer support via telephone, email and online chat.

Parentline www.familylives.org.uk run by Family Lives (help and support in all aspects of family life)

helpline@saferinternet.org.uk being created by SWGfL for professionals (such as teachers) who work with children to provide cross UK support, advice and mediation with online safety issues.

Based Outside the UK

Insafe www.saferinternet.org/web/guest/home;jsessionid=83E3203621732A5C53BAEC3379A1EE0C EU network of Awareness Centres

Safe Kids www.safekids.com: The Online Safety Quiz is your chance to show that you know how to be a safe Internet surfer. Answer each question and, when you get it right, you'll go to the ...

Family On-Line Safety Institute www.fosi.org : US based global consortium, membership includes main US fixed and mobile operators and Internet service providers plus BAE-Detica, BT and Telefonica,

GetNetWise www.getnetwise.org : Online Safety Guide produced by Internet Education Foundation backed by Verisign, e-Bay, Google and Microsoft, also secretariat for Internet Caucus in Washington.

Digital Mom www.digitalmomblog.com/blog/2010/02/23/kids-the-internet-and-boundaries/

3) Professional

Top Tips on Security for IT Professionals www.bcs.org/category/15291 with links to reputable web sites

CESG Top Tips series www.cesg.gov.uk/Finda/Pages/PublicationResults.aspx?cat=All&term=Top+Tips

CPNI Guidance http://www.cpni.gov.uk/advice/ and http://www.cpni.gov.uk/advice/cyber/

Security Awareness Special Interest Group www.thesasig.com those running staff awareness programs

4) Directors/Executives

Directors Guides www.theisaf.org/kzscripts/default.asp?cid=9 Information Security Awareness Forum

CESG Executive Companion www.bis.gov.uk/assets/biscore/business-sectors/docs/0-9/12-1120-10-steps-to-cyber-security-executive.pdf

BIS10 steps to cyber security http://www.bis.gov.uk/policies/business-sectors/cyber-security/downloads

5) Small Firms

Bobs Business www.bobs-business.co.uk The only awareness operation targeting SMEs, spun-off from a mid-Yorkshire Chamber of Commerce programme with BIS funding

IASME (Information Assurance for SMEs) Consortium www.ncc.co.uk/services/accreditation/iasme/ certification programme for organisations with less than 250 staff

National SME Segmentation 2012 www.homeoffice.gov.uk/publications/agencies-public-bodies/nfa/sme-fraud-segmentation analysis of SME attitudes and behaviours toward fraud and internet

Business Link IT Security and Risk
www.businesslink.gov.uk/bdotg/action/layer?r.s=m&r.l1=1073861197&r.lc=en&r.l3=1075406921&r.l2=1075408323&topicId=1075408323

6) Silver Surfers

Confidence to say “NO” National Consumer Week – November. TSI/www.tradingstandards.gov.uk co-ordinated campaign due to include exercise to help adults aged 56plus, recognise fraud with support from   OFT, Age UK, FFA U

7) Commercial operations running awareness exercises for customers (large and small)

The Security Company International www.thesecurityco.com the first UK-based company to focus entirely on running awareness campaigns for the staff of medium to large organisations.

The Security Awareness Company www.thesecurityawarenesscompany.com 20 year old US company running corporate awareness Programmes

Terranova www.tnawareness.com 10 year old Canadian company trained over 2 million corporate staff, including via delivery partners in the UK/EU

Securing the Human www.securingthehuman.org the awareness operations of the SANS institute

SAI Global http://www.saiglobal.com 90 years old Australian security and governance consultancy

Online E Safety redstor.com www.redstor.com Hosted e-safety monitoring for schools
K, CAB, MPS, Royal Mail, Charity Commission, Victim Support