

Technical Appendix to Annex 3

e-Security and Investigation Skills: A Joint Responsibility - but for whom?

1 Background

In May 2004 “Supplying the Skills for Justice” www.eurim.org.uk/activities/ecrime/skills.pdf was published as part of the EURIM- IPPR study into “Partnership Policing for the Information Society”. That study called for government and industry to co-operate in organising “awareness” programmes but warned that these could be counter-productive if not followed up by training and support programmes at every level: from basic self-protection for end-users through operational security and victim support to the higher level skills to design out vulnerabilities and to track, trace, remove/deter (and perhaps even convict) criminals.

Since then the UK has had successful awareness programmes on E-Crime, On-line Child Protection and ID Theft but the 2007 Oxford Internet Institute Survey www.oii.ox.ac.uk/microsites/oxis/ found that barely one in five of Internet users had received any training. Most “work things out for themselves” or ask friends, family or work colleagues. At the other end of the scale, the then DTI-supported Cybersecurity Knowledge Transfer Network annual conference was told the UK was the best place in the world to research information security issues, but was no longer the best place to recruit graduate researchers.

The recent House of Lords www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf report on Personal Internet Safety commented that “Government’s well-intentioned efforts to raise *awareness* of e-crime, without paying enough attention to the ways in which individuals or businesses can protect themselves against it, are actually making the problem [of confidence in the Internet as a safe place] worse”. This led it to call for Government and Ofcom to support “Get Safe Online” as a common Internet security “portal” and for the Department for Children, Schools and Families to find new ways of educating adults, as well as children, in online security and safety. Many of the report’s other recommendations have implications for the skills needed by industry and across law enforcement and regulation.

2 Who says who needs to know what?

Skills requirements are commonly defined as rungs on ladders. Thus the bottom rung on the “personal e-protection ladder” might be: “basic security awareness, the ability to use pre-installed mass-market security facilities and to know where to go for help”. The next rung might be the skills that system retailers and their support staff need in order to install those facilities and provide such help to paying customers. And so on. Similarly the bottom rung on the “Information Assurance” ladder might include the skills needed by those working in call centres or hospitals to check the authorisation of those claiming right of access to customer or patient information. Higher rungs for those running corporate systems, including those to service on-line enquiries and transactions, might include the skills to ensure that existing products and services are configured securely and that new products and services do not contain unnecessary vulnerabilities. Other ladders might include those for “Risk Assessment”, “Investigation” et al.

Most on-line crime is, however, old crime exploiting new media. Technologies are evolving and consumers are migrating across delivery channels (fixed, mobile, wireless, broadcast etc.), let alone using products and services in ways the suppliers did not predict. Moreover most of those needing skills in this space are not following career development programmes to become information security (or other) professionals. Therefore the ladders and rungs have more than one dimension, change over time and/or lead nowhere predictable. Indeed they may be more akin to the moving staircases in The Hogwart’s School of Witchcraft and Wizardry than the career development paths of a traditional trade or profession.

So who is involved in trying to define the skills needed by whom, the courses and qualifications to help acquire them acquire those skills and the accreditations that might indicate the knowledge and abilities that school-leavers, job applicants or consultants possess?

2.1 UK and International Requirements

The UK Accreditation Service www.ukas.com is the only UK body officially recognised to assess organisations that certify, against internationally agreed standards, the competence of individuals or the processes of organisations providing services such as quality assurance or the provision of training. It currently has no regimes specifically for electronic security, investigators, computer forensics experts and the like, although EN45012 is for those assessing quality systems “modified for Information Security Management Systems”. 19 UK organisations are registered as assessors and several of these offer services with regard to ISO17799 and ISO27001(based on BS7799) for security management. ISO 17024 is the standard for those operating the certification of individuals. Those running the most widely recognised security qualifications (see below) have accredited these using ANSI, the US-based equivalent UKAS.

The Quality Assurance Agency www.qaa.ac.uk benchmarks the processes used for setting and assessing higher courses and curricula. The Qualifications and Curriculum Authority www.qca.org.uk approves courses and qualifications for UK public sector funding. It recently conducted a consultation to update the ICT components of key stage 4 in schools. The submissions included proposals covering on-line safety and security. The House of Lords called for a similar exercise regarding adult skills, including those of parents to help protect their children. The skills definitions to be used for such an exercise, including updates to add Internet safety to current publicly funded end-user IT courses, would fall within the remit of the Sector Skills Councils. These maintain the “National Occupational Standards” used by QCA to approve adult qualifications and courses for public funding.

“Skills for Security” www.skillsforsecurity.org.uk has produced standards for generic risk management and security (i.e. alarm) systems. “Skills for Justice” www.skillsforjustice.com (which covers law enforcement, prison, courts etc.) has approved standards for investigators but these have yet to be turned into courses and qualifications. “E-Skills”, www.e-skills.com (the sector skills council for the computing, information technology and telecommunications industries and their users) has a project, to update the standards for electronic security consultants. The ICT occupational standards map onto a more detailed set of standards maintained by the SFIA Foundation (Skills Frameworks for the Information Age) www.sfia.org.uk. SFIA is owned jointly by e-Skills and the main UK ICT professional bodies: BCS, IET and IMIS. The SFIA standards are used by many large ICT employers to plan staff training and development and include definitions for Security Administration and for Information Security as a whole, at levels 3 (technician) to 6 (setting corporate policy). The British Educational Communications and Technology Agency www.becta.org.uk also provides more detailed guidance to schools than is mandated in the Key Stage standards. It is unclear who uses the QCA occupational standards other than to apply for public funding.

2.2 Professional and Technical Standards, national and international

There is a wide range of product-specific certifications available in UK and Europe, relating for example to Microsoft, CISCO and similar products. These certifications relate to specific abilities to configure and manage those products and their security features.

The main “non-product-specific” certifications, in order of “recognition” (see section 3) are those from:

ISC2: International Information Systems Security Certification Consortium www.isc2.org , over 50,000 individuals certified in 129 countries (including more than 2,300 in the UK). The certifications include: **SSCP** (Systems Security Certified Practitioner) and **CISSP** (Certified Information Systems Security Professional, based on a 250-question multiple-choice examination - this is the one most recognised).

ISACA: Information Systems Audit and Control and Control Association www.isaca.org , 65,000 in over 140 countries including **CISM** (Certified Information Security Manager for corporate security and risk managers, peer references and examination: 4th) and **CISA** (Certified Information Security Auditor: 2nd).

ISEB: Information Systems Examinations Board www.bcs.org/server.php?show=nav.5732. These include **CISMP** (Certificate in Information Security Management Principles - an entry level certificate; based on a

100-question multiple-choice examination: comes 3rd in recognition by UK security professionals) and **CIRM** - Certificate in Information Risk Management a full professional certification course (new course).

GIAC “Global Information Assurance Certification” www.giac.org was founded in 1999 “to validate the skills of computer security professionals” for the United States National Security Agency and other US government agencies and private sector bodies. GIAC has certified 18,000 professionals who have to submit a technical review paper and take update exams every four years to demonstrate specific skills and knowledge for its “Silver”. Those aspiring to “Gold” also have to submit a technical review paper. GIAC comes 4th equal in recognition in the UK.

ITPC Infosec Training Paths and Competencies www.cabinetoffice.gov.uk/infosec for UK Government, its agencies and contractors. This is mandatory for accreditation in the CESG List Advisor Scheme www.cesg.gov.uk/site/clas/index.cfm. Despite such support ITPC is well below GIAC in “recognition”.

The more specialised certification schemes currently in development include those of CREST, The Council of Registered Ethical Security Testers www.crest-approved.org, for penetration testers, and the Tiger Scheme, for secure document management (see www.oursizes.net/status/default.asp for current status).

The mainstream ICT professional bodies have special interest groups and registers covering information security. Thus the BCS has a Security Forum which has special interest groups covering information systems security (www.bcs-issg.org) and information risk management www.bcs-irma.org. The BCS also provides the secretariat for the Information Assurance Advisory Council www.iaac.org.uk which describes itself as a “centre of excellence in the UK and Europe for the provision of policy recommendations on information assurance. The UK Council for the Registration of Forensic Practitioners covers those capturing and analysing basic data from PCs, but has no registers for those analysing communications data or that from networked or complex systems www.crfp.org.uk/specialties/specialties/computers

Many security related groups have called for action to address particular on-line safety, security and investigation skills with objectives from informing/changing end-user behaviour through developing and recognising technical or professional competence to changing the attitudes and priorities of senior management. They include trade associations and practitioner groups like: the Alliance Against Counterfeiting and Piracy, the High Technology Investigators Association, the Information Security Forum, the Internet Enforcement Group, the Mobile Industry Campaign Against Fraud, the Risk and Security Management Forum, the Security Professionals User Group and the Telecommunications UK Fraud Forum.

The Institute for Information Security Professionals (IISP) www.instisp.org was created to avoid pressure for electronic security professionals to come within the remit of the Security Industry Authority www.the-sia.org.uk/home and was supported by Cabinet Office to aid the career development of those working on secure systems for central government. The initiative also addressed a private sector need and is currently supported by around 30 large employers of security professionals (both public and (private sector). It has a thousand associate members and has started the process of accrediting full members. The founding members, who include those responsible for the security of much of the UK critical financial, business and economic infrastructure, have spent much time and effort assembling a “body of knowledge” to underpin the accreditation process and to aid the creation of detailed professional development programmes for their staff and successors.

The active membership of the UK chapter of the Information Systems Security Association www.issa.org (around 14,000 members world-wide, 1,100 in the UK) overlaps with that of the new IISP and of ISC2, ISACA etc.. ISSA does not, however, do accreditation. It is more concerned to bring together those accredited by others for mutual education and action programmes. ISSA is currently planning to involve its members in e-crime prevention programmes linked to the Get Safe On-line campaign. Meanwhile ISC2 encourages those it accredits in the UK to help Childnet www.childnet-int.org deliver its schools education programmes.

At the technician level the most widely recognised qualifications appears to be “security +” produced by COMPTIA www.comptia.org, the US-based Computing Technology Industry Association, set up in 1983 to

improve the skills of dealer support staff and now supported by almost all the main US suppliers The basic COMPTIA qualification for technical support staff, A +, also includes basic security skills.

2.3 Law Enforcement Skills

At one time the NSLEC Centre for National High Tech Crime Training was said to account for most of the training in e-crime skills for law enforcement. The operation was transferred to the 'National Centre for Policing Excellence – Specialist Training' (nh2tc.org) which has (since April 2007) been subsumed by the National Policing Improvement Agency. The NPIA high tech team www.npia.police.uk/en/5236.htm currently runs a "First Responder" course, a Masters in Cybercrime Forensics and some more specialist courses. Some forces have arrangements with local Universities to provide first responder training to all recruits as well as tailored higher level courses, including MSc programmes. Several use packaged and on-line material (including from Australia, Canada and the US) in their in-force training centres.

2.4 End-user Skills: from consumers to retail and administrative staff

There are many (too many) ICT end-user qualifications but the most widely used, the "European Computer Users Driving License" (ECDL) contains only rudimentary material on computer security, not updated in recent years and outside the assessment process. Most of the others contain little or nothing. There is an attempt (led by E-Skills) to establish a common "skills passport" which may indicate not only what general IT qualifications, but also what security training, if any, the individual claims. The only end-user qualification known to cover on-line safety, self-protection and good citizenship is the Scouting Association Award, supported by BCS and now held by over 40,000 scouts and guides.

Most UK retailers have now upgraded to accept chip and PIN cards and the "Spot and Stop Card Fraud" education pack and training programme, developed in collaboration with retailers, police and organisations like Crimestoppers, is probably the largest single UK fraud prevention training programme to date. An online version of the training pack and a DVD to complement the training programme are available at www.cardwatch.org.uk.

APACS, the UK payments association, www.apacs.org.uk, the British Bankers Association www.bba.org.uk and CIFAS www.cifas.org.uk, with Home Office backing have also produced online training www.idfraudpreventiontraining.com with best practice guidelines for businesses that could be targeted by identity fraudsters. This features an interactive learning section to improve the understanding of employees who need to check and verify the identity of customers on a day to day basis.

Many large organisations, especially in the financial services, provide mandatory training on basic systems security, including data protection, to all staff. This is often linked to BS7799 (ISO17799/20001) and other regulatory, governance, certification and accreditation processes. Some organisations do not permit new users to log on until they have successfully completed an assessment of their skills - including, for example, how to check the identity and authorisation of those seeking access to customer data. Some also require regular update training and assessment as part of password renewal processes. Those providing such training in on-line form may also make it available to the families of staff.

However, even though the customers of security consultancy and training suppliers such as Detica, Qinetiq and Siemens Insight may have put hundreds of thousands of staff through very similar programmes, there are no known shared certifications or plans in this area.

2.5 Educational, Academic, Research and Development Skills

Information security and on-line safety are not currently well covered in most UK undergraduate computer science or business IT courses, although this is beginning to change with the new courses planned by a consortium of employers and universities through E-Skills. Also at least five Universities now offer undergraduate degrees in ICT Security (various titles) and/or Forensic Computing. Most students are also offered basic security training when they sign up to the university network but this is rarely mandatory.

There is a growing number of MSc courses covering varying mixes of information security and forensics. EURIM published a grid of these www.eurim.org.uk/activities/ecrime/Univgrid.doc in late 2004. A programme is under discussion which will enable this to be updated as part of a project, supported by the Cybersecurity Knowledge Transfer Network www.ktn.qinetiq-tim.net, to identify which organisations have relevant skills and potential, not only with regard to e-security research and development, but also to transferring the results to the benefit of the wider UK economy via skills and training programmes.

There have been various attempts to create modular degree courses with standardised and co-ordinated content but these do not yet appear to have been successful. The main linkages between those running degree courses appear to be via the exchange of external examiners and/or shared research projects.

3 Who currently requires/teaches/trains/tests/accredits what

Information Security Solutions www.informationsecuritysolutions.com, which provides recruitment services to some of the UK's largest employers of information security staff, has just surveyed the qualifications and accreditations required by employers and those which security professionals believe enhance their careers. The most significant finding of the study is, however, that the average salaries on offer to information security professionals, from administrators through consultants to chief information security officers have risen by around 25% since 2004. In that period the salaries on offer to IT professionals in the private sector have gone up by under 10% (i.e. below inflation).

87% of respondents thought that qualifications would help with promotion or getting a new job and they found nearly fifty qualifications. Only seven were, however, said by respondents to be of value to them: MSc - 44%, CISSP (ISC2) - 17%, MBA - 10%, CISA (ISACA) - 10%, CISM (BCS) - 7%, CISM (ISACA) - 3% and GIAC - 3%. The MSc and MBA courses mentioned were those of: Cranfield, De Montfort, East London, Glamorgan, Royal Holloway, Portsmouth and Westminster. Over 80% of respondents were also active in the industry's many security forums. The most popular six, in alphabetical order, were: the BCS - British Computer Society, IBSIG - the Investment Bankers, IISYG - the Independent Information Security Group, ISACA - the Information Systems Audit and Control Association, IISP - the Institute of Information Security Professionals and ISSA - the Information Systems Security Association.

The list of qualifications and degree courses overlaps with those recommended on the website of Barclay Simpson www.barclaysimpson.com/content_static/information_Security_summary_of_qualifications.asp, who have been recruiting for Corporate Governance posts, including security, since 1989 but there are some interesting differences, including the Universities named and the value given to accreditation by GIAC (mandated by US Federal agencies) rather than ITPC (mandated by HMG).

The US-based SANS Institute <https://www2.sans.org> claims to be by far the world's largest security training organisation. It offers a wide variety of courses, including in the UK. UK-based organisations with large security consultancy practices, like Detica, Qinetiq and Siemens Insight, also offer generic information security courses based on what they deliver to their own staff and to regular customers. The main ICT training providers, the short course operations of those Universities offering security and forensic degrees and several dozen security consultancies also offer commercial security courses leading to the most popular vendor independent (e.g. ISC2, ISEB, ISACA, and Comptia) qualifications and the vendor-specific certifications in most demand (e.g. Microsoft, CISCO etc.).

In aggregate, these certificates cover a wide range of security training activities - from how to use the security facilities already built into mainstream operations, through the use of specific forensic analysis to how to investigate crime which makes use of e-Bay transactions, provided free to law enforcement by eBay itself and available to others via www.ecops.co.uk. However, no-one has done any gap analysis.

4 Summary

It is unclear who is responsible for specifying which skills are needed by whom, let alone for accrediting or delivering them. That will complicate any attempt to comment on how far the content of the training on offer meets the needs of employers, managers, professionals, technicians or end-users.