



**Report of the EURIM Personal Identity Subgroup meeting, 23 March 2005,
1200 – 1400 Room P, Portcullis House, Westminster**

Chairman: Jim Lound (Experian)
Rapporteur: Dave Wright (EURIM)

SUMMARY OF MAIN POINTS

1. The purpose of the meeting was to see whether there is potential agreement for a short paper on the need to improve practice, produce common guidelines and/or standards, enforce these with regard to public sector systems and commend them to the private sector.
2. John Walker as chair of the BS 7799/ISO9000 group and vice-chair of the EURIM e-Crime Group focusing on reducing vulnerability, gave an introductory talk on public sector databases and security routines. JW identified a serious shortage of technical skills, and the need to understand the nature and scale of the problem, as the major issues; attempting to fix the problem without understanding the issue is probably responsible for the current failure of information management across both Government and industry.
3. After the General Election, EURIM has the opportunity to produce briefing material for the intake of new MPs. Simple recommendations on the do's and don'ts regarding databases for Government departments dealing with citizens online or otherwise will resonate with MPs, who may then gain an understanding of the importance of the general issues. Generic, high-level educational material has the potential to make a major impact through a common appeal.
4. Security awareness and testing is the key to solving many of the problems: most current advice routines for online security are written by experts for experts - thus negating their usefulness to the vast majority of users. Even downloading software from security vendors often conflicts with good practice by requiring certain at-risk programmes to be enabled on the user's PC. Operators, officials, industry etc. need an overarching standard as a fundamental prerequisite for solving the problem. A EURIM paper on this topic would add value to the debate.
5. Surveillance and hacking tools readily available on the Internet are frequently used to breach security and mount attacks, and the user needs to be aware of these possibilities. Schemes that notify an individual when their credit record has been accessed offer additional protection.
6. Less than 40% of UK companies have a security policy, and only 1 in 25 CIOs do risk assessments. Scenario-based risk assessments that define policy and lead to procedures, standards and guidelines in the architecture are necessary to provide meaningful security; awareness programmes, not more technology, are needed, and BS 7799 would be a good starting point.
7. Standards, good governance and good practice, including scenario-based risk assessment exercises, are available but have generally not been used; the implementation and enforcement of good practice is the key issue to address, and requires a political framework that assures this.
8. EURIM is now planning a programme to help promote the message that standards and information assurance for the public sector are needed, and will call for support from eGU and CSIA.

1. Introduction

1.1 The purpose of the meeting was to see whether there is potential agreement for a short paper on the need to improve practice, produce common guidelines and/or standards, enforce these with regard to public sector systems and commend them to the private sector.

1.2 John Walker, as chair of the BS 7799/ISO9000 group (and vice-chair of the EURIM e-Crime Group focussing on reducing vulnerability), gave an introductory talk on public sector databases and security routines. (British Standard BS 7799 sets out the requirements for information security management systems. It helps identify, manage and minimise the range of threats to which information is regularly subjected).

2. Background to the meeting

2.1 The idea for this meeting emanated from the Foundation for Science and Technology meeting on Identity Management on 23 February. At the dinner, Philip Virgo as Secretary General of EURIM briefed Ian Watmore on the activities of the EURIM Personal Identity Group.

2.2 Before IW's appointment, PV had been asked to help focus attention on public sector information governance, because of the variability of actual practice and apparent lack of common guidelines. The central question is: 'what is, or what should be, good practice in Government dealings with citizens, and how could this be made more secure?' A further question is 'How can eGU promote good practice, and how can EURIM help?', given that eGU needs to have the ICT professional bodies and other stakeholders calling for better practice so that eGU can respond. This is because eGU is not an executive body and cannot mandate implementation of any policy; rather its aim is to re-professionalise the Civil Service by encouraging adoption of best practice and guidance, and to reduce the likelihood of bad practice through political expediency.

2.3 A similar exercise on simple security guidelines for SMEs had been undertaken within EURIM on e-Crime; the guidance was now posted on the NHTCU website. Funding from the Welsh Office had made this possible! The first use of the draft guidelines had been within one of EURIM's corporate members, where they had been used to help educate the main Board as a simple example of the challenges faced by the smaller organisations in their supply chain before the Board set the security budget for the organisation itself.

2.4 Examples were given of supposed phishing attacks from telcos and banks that had proved to be genuine messages sent by contractors working for their marketing departments using non-proprietary websites. Referring the 'attacks' to the security sections of the organisations concerned caused a certain friction between the security and marketing departments! The question however is, where is the guidance on communicating with customers, and who is responsible for producing it?

2.5 After the General Election, EURIM has the opportunity to produce briefing material for the intake of new MPs. This could include a simple draft on the do's and don'ts regarding database access and updating for Government departments dealing with citizens online or otherwise. How do you check that an application for a change of name and/or address is genuine? BS 7799 might hold the answers to some of these questions. Ian Stewart MP (Chair of the EURIM Content and Issues Panel) might well wish to see the briefing included in any resource pack for exercises to help educate new MPs and their research assistants.

2.6 CESG might be expected to have an advisory role in security guidance, given that current practice is not adequate for purpose. However, CESG guidance is much more detailed at the operational level, and in any case most departments were unaware of the services it could offer. A joint EURIM-CESG event in November 2004 on the large-scale roll-out of biometrics had been very successful, and although very few MPs attended there had been over 70 attendees from across central government to hear the message that all Government departments could approach CESG for advice on information security. Coverage of the main topics is available on the CESG website at: (http://www.cesg.gov.uk/site/ast/biometrics/media/BWG_Slides_CESG-Eurim25Nov2004.pdf).

3. Introductory talk on public sector database security routines

3.1 On issues of information security, we need to understand the landscape before we can solve the problem; attempting to fix the problem without understanding the issue is probably responsible for the current failure across both Government and industry.

3.2 The Internet itself is part of the problem – a lot of hacking software is readily available, and many people do not realise that the search engine Google can act as an effective hacking tool! Google can be used to gain access to personal information on web servers, e.g. telephone numbers, passwords etc. Using a proxy server conceals the true identity of the attacker, and allows the user to indulge in criminal activities without detection. This raises a major question: should a site owner accept connections from a proxy server? Why do people want to anonymise their identity?

3.3 The answer to this goes back to the origin of the Internet; it was designed to facilitate anonymity. It is not possible to ban anonymous users or close anonymising sites down because you have to accept that they are going to be there. But who would want to receive a connection from an anonymised user? The trouble is that if access was prevented, systems would become smart enough to appear to originate from a bona fide identity. It was agreed that anonymity presented a problem.

3.4 The shortage of technical skills is a second major issue, with a serious personnel imbalance compared with e.g. compliance. As an example, a recently promoted law-enforcement website was readily caused to default to a maintenance page holding confidential details, showing that due care was not applied during the construction of the site. Some police websites still require visitors to use technologies like Flash which can be easily compromised. Controls in place on information owned by the police also gives cause for serious concern – in some cases, details of people under protection were stored on open-access systems. Systems administrators typically on £9000 pa could be exposed to bribery from wealthy criminals, and the issue of security generally has too low a priority. This is part of the landscape that we have to understand before effective solutions can be implemented.

3.5 Some of the voluntary organizations concerned with child welfare and other vulnerable groups face similar problems. . An example concerns the records for a programme to rehabilitate abusers who were themselves formerly victims. In such cases it may be that the only way to ensure adequate and credible security is to store files on non-networked computers without Internet access or on paper files locked in safes.

3.6 However, security can only be limited – every Western defector had been vetted! British Library plans to catalogue all the websites on the Internet is an example of information being stored on web servers where administrators are unaware of its existence, and that it is accessible. A knowledgeable user could access that information e.g. through Google. Many tools available on the Internet, such as cracking kits, reverse engineering telephone codes etc. enable illegal activities.

3.7 A key issue is the standards in place. Good security practice requires turning off Java or ActiveX when accessing the Internet for downloading software, but downloads from security vendors often require these to be enabled, conflicting with good practice! Awareness is a key requirement, by developers, users, citizens and Government.

3.8 Authenticating the identity of someone you are speaking to on the phone is difficult. Similarly, examining the credentials of a utility worker, or even a police warrant card, presents problems, since most citizens have no standard against which to compare it, and have probably not seen the genuine article before.

3.9 One suggestion was to test the credentials of public sector requestors applying to access your home or business by using a well-publicized routine to ring a unique number (the equivalent of Whitehall 1212). The receptionist would then give the caller a test question designed to verify the identity of the requestor. This had been suggested as the first pilot use for ID cards, mixing electronic and physical security.

3.10 Awareness is another key to solving many of the problems. Authenticating to your bank is one-sided – the citizen is required to furnish the bank with identity credentials, but with few exceptions, not vice versa. Two sets of data should be required in such a reverse identity-authentication routine, so that more than one set of credentials can be used to permit access to an individual's account.

3.11 How does a user know he is working with a business and not a phisher? An answer is to ask the user to undertake a DNS lookup, look at the MX record, do a reverse DNS check and identify the IP number, and then see if it's the person you wish to trade with. The assumption here is that the user is an expert, and this is patently not the case. The advice routines are written by experts for experts - thus negating their usefulness to the vast majority of users, and online security becomes a joke.

3.12 Web-enabled services proffered by Government and industry fail to provide adequate information for users to go online securely. Security testing is a rarity, e.g. very few people set the database on their server to show if a web-crawl has taken place. How do you protect the user base? Perhaps the organisation's reputation is more important, but e.g. in the USA, California law now requires firms to disclose unauthorised access incidents to the client base when they are discovered. Thus ChoicePoint recently notified between 30,000 and 35,000 consumers in California that their personal data may have been accessed by unauthorized third parties. The wider use of such laws may start to reverse the way Governments and organisations think about breaches of confidentiality and data theft, and concentrate minds.

3.13 Similarly, California Law SB 168 (Debra Bowen) prevents identity theft by taking Social Security numbers out of the public's view and the easy reach of criminals by making it illegal for businesses to do any of the following for new accounts after July 1, 2002:

1. Post or display Social Security numbers;
2. Print Social Security numbers on identification cards;
3. Require a person to transmit a Social Security number over the Internet unless the connection is secure or the Social Security number is encrypted;
4. Require a person to use a Social Security number to log onto an Internet Web site unless used in combination with a password or other authentication device; and
5. Print a Social Security number on any materials mailed to a customer, unless it's required by law, or the document is a form or application.

SB 168 also prevents identity theft by giving people the right to 'freeze' access to their credit reports. Placing a security freeze on your credit reports means an identity thief – even one who has your name, address, Social Security number, birth date and more – will not be able to get new loans and credit in your name. That's because lenders, retailers, utilities and other businesses need access to a credit report to review and approve new credit, loans, and services.

Experian's 'credit expert' scheme, which informs an individual when their credit record has been accessed, offered similar protection.

3.14 Even with a secure website, and using encryption to log on to their online bank account at an access point, if a wi-fi access point is used, a "promiscuous" network card in a PC can be used to 'sniff' or detect the users credentials, account numbers and password. Keylogger surveillance tools (both hardware and software) that record every keystroke to reveal passwords etc. are another potential means of breaching security. The end-user needs to be aware of these possibilities.

3.15 In conclusion, **security awareness is a key issue**. Operators, officials, industry etc. have no benchmark for guidance, and **overarching standards are a fundamental prerequisite for solving the problem; a EURIM paper on this would add value to the debate**.

4. Discussion

4.1 On the issue of wi-fi communication, there is probably no security implication for wireless mice and keyboards because their wireless range is very short.

4.2 A talk at the CMA conference in February had advocated a 'deperimeterisation' approach which some believed would reduce the need for IT directors to manage secure access to a network. This proposal is a theoretical approach and although still immature, some thought that it may develop into a workable, scaleable solution. Others argued that the only practical approach in the extended perimeter environment was through compliance and regulation. However, although compliance and regulation are good business drivers for security, and not inconsistent with deperimeterisation, bounded perimeters on the Internet are not feasible when anonymity is permitted. As long as business wants to use the Internet as a major channel for transactions, there will be security problems.

4.3 The Internet is multi-track, multi-speed and embraces a wide variety of types of network, not just digital packet-switched: 'anonymous any-to-any' is really a subset of it. There are secure protocols within the Internet, and business has to decide whether it is happy to use an uncensored environment

where anonymity is accepted, or whether business uses a secure subset, in which it can refuse unauthenticated traffic. The latter raises questions of whether absolute authentication is possible, but at least routines can be improved.

4.4 The Internet had evolved from its libertarian/academic roots into becoming a global reliant system for Government and business communications, raising serious questions about how to control its continued development. Businesses want to use the Internet is because it offers a cheap and direct method of communication; using a subset would restrict the target audience. However, there are a number of different approaches, e.g. ISOC communicates by raw text emails – the lowest common denominator and hardest to falsify. Was that because ISOC wanted to be socially inclusive, or because it has members who don't trust anyone?!

4.5 If a Government department wished to offer a new service, could it not launch a website to permit anonymous interactions that used a registration process that establishes identity? Post registration access would then be exclusive, offering in effect 2 levels of service? This is the case for most public websites, but the degree of restriction depends on the rigour of the registration process, and the amount of risk the provider was prepared to accept. At least 10% of the population did not have a reasonably fixed abode, and were therefore likely to be excluded by registration; on the other hand, registered users' home systems, let alone their portables, could be spoofed.

4.6 VoIP has created a new market space for selling IP addresses on insecure servers in corporate space that provide free access to telephone calls. Communication is now network rather than telephony. If network replaces direct channel telephony, authentication could be in doubt, because calls can be hijacked and re-routed on the network to imposters - this would be even more probable in cases of subcontracting.

4.7 Scenario-based risk assessments that define policy and lead to procedures, standards and guidelines in the architecture are necessary to provide meaningful security. Unfortunately, most companies give insufficient attention to security because of cost and lack of awareness: less than 40% of UK companies have a security policy, and only 1 in 25 CIOs perform risk assessments; meanwhile, the scale of e-crime is probably massively underestimated. The need for physical security is readily understood, but digital security is more complex and subject to unseen, sophisticated attack methods. **We need continual awareness programmes, not more technology, because hacking techniques are continually 'improving'; BS 7799 would be a good starting point.**

4.8 Different cultures within an organisation often lead to conflicts of interest, particularly between marketing and security, and these increase vulnerability. Marketing by emails with graphics might be eye-catching, but increases security risks. CRAM (Committee on Risk Assessment Methodology) method was ineffective, and could actually cause harm. Risks need to be thought through in the work environment, including different departments, not in isolated classrooms. **Scenario-based risk-assessment, not tick-box assessment, is necessary to minimise risk and enhance security and awareness.**

4.9 The Skills for Justice workshop on 30 March will focus on specifying skills such as risk assessment. Part of the Sector Skills Council, the group is producing the national skills framework for specifying e-security skills in general. Consultants have a budget to assemble a skills grid for the criminal justice system, matching jobs to skills requirements. Two members at the meeting volunteered to help.

4.10 A practical solution to security concerns would be a new approach to security on the Internet, with more intelligent devices and enforcement points, and networks that select permitted communications, similar to VPNs, etc. Trust was the fundamental driver in security; in the physical world, you could build trust with people you know, but in the digital world, trusted intermediaries offered a similar solution to assurance of trustworthy services. However, while third parties who accept liability may win trust, most of the electronic trust models *avoid* liability! This is why banks are hurting, because they indemnify a genuine user against loss due to fraud.

4.11 Standards, like BS 7799, Proteus, etc. are available but often unused; the different standards need to be aligned so that the industry has a common standard and can develop mechanisms and build architectures in an appropriate way. Interestingly, the Government had originally rejected the BS 7799 approach. However, no group in Government could actually impose solutions across Whitehall, let alone elsewhere. Thus the eGU team of CIOs is attempting to rebuild professionalism with career

paths etc. on the lines of the old CCTA (from 1st April 2001, CCTA became an integral part of the Office of Government Commerce), and to widen its sphere of influence.

4.12 There are a number of problem spaces and audiences that involve both common and specific messages through different channels, together with questions about who should do what. EURIM can network across Government at different levels according to the task. Generic, high-level educational material for the new intake of MPs has the potential to make a major impact through a common appeal. Simple recommendations for dealing with the public will resonate with MPs, who will then also begin to gain an understanding of the importance of the general issues. Other more high-level issues sit with DTI, FSA, Home Office etc. as well as with their various departmental and sponsored regulators.

4.13 The application of good governance would include risk assessment, so that decisions could be taken about what risks are acceptable, and those that require mitigation. Why then did public sector systems encounter difficulties, when good governance and good practice has been established for many years? **The issue is, why is good practice not followed, and how can it be enforced? Implementation requires a political framework that assures adequate embarrassment for failure to follow good practice.**

4.14 Shorter timeframes work against implementation of good practice. Audits and compliance requirements at Board level, with Board accountability, have improved awareness and expenditure on IT security, but has operational security had actually improved – or had companies become good at passing audits? Although auditors are now looking at access and security issues because of Board level liability, audits can encourage people not to get caught, when the need was to encourage them to comply. Are auditors actually skilled for the job? Banks have a fundamental role to play; at the moment they were plugging holes but the security issue is rising rapidly up the agenda.

4.15 **The implementation and enforcement of good practice is a key issue for the EURIM subgroup to address, and an essential part of that is to identify the relevant audiences and the points of leverage.** The subgroup should then define:

- which messages should be sent to which audiences,
- which channels should be used to reach the audiences, and
- which players should be involved in delivering the messages.

Awareness and communication of the problems (not the solutions!) are therefore central to the message. Detailing how to communicate simple methodologies of risk assessment, and who within an organisation should be involved, would add value. Technology issues are probably better addressed elsewhere (e.g. Skills for Justice).

4.16 An exercise akin to that by EURIM-IPPR-NHTCU on SME's, on how to deal securely electronically with your customers in a small firm, might be most appropriate. Within the public sector, we might wish to involve CESG in a security workshop with a key aim being to inform security people in the public sector of contacts within CESG who can help for particular services. We need to sell the idea that standards and information assurance for the public sector are needed, and that eGU should support getting this set up, with Treasury sanctions for those who fail to respond.

4.17 Dave Wright would contact eGU/CSIA with regard to this subgroup's future actions, and also CESG contacts with a view to a joint workshop.

5. Date of next meeting

5.1 The date of the next meeting will be 4 May 2005, but a rapporteur would need to be found, as DW would not be available.