



Report of meeting of the E-Crime Sub-Group on Reducing Vulnerabilities held on Tuesday, 7 September 2004, at 1000-1200 hours in Room 'P', Portcullis House, Westminster

SUMMARY OF MAIN POINTS

1. The aim of the meeting was to review the recommendations of the February 04 version of the EURIM-IPPR working paper 'Reducing Opportunities for E-Crime', which should be read alongside this report.
2. Some recommendations have already been accepted, and if the timetable is met, ministers can be expected to respond. Outcomes of the meetings this month should include the publication of discussion papers and recommendations by October or November. The forthcoming series of industry events on Information Security will provide platforms to put the recommendations onto the political agenda and into the manifestos of the main political parties. A major event with IPPR, with a ministerial response, is planned for early February 2005.
3. The working paper considers reducing opportunities for e-crime in a number of different ways, through:
 - education and awareness;
 - managing risk and building trust;
 - looking at commercial opportunities;
 - looking at technical solutions.
4. Security should be promoted through the supply chain, with adherence to three principles:
 - security should be easier than insecurity;
 - security should be cheaper than insecurity;
 - security should be a community issue.
5. Recommendations 1-6 are removed, because they were included in Discussion Paper 2 and should be addressed by Project Endurance, a Government-Law Enforcement-Business initiative to coordinate public and SME awareness of the importance of security, and what needs to be done.
6. There should be a recommendation that the relevant professional bodies should work with the Sector Skill Councils to include risk assessment in skills sets and training programmes. There should also be a recommendation that the Turnbull report be updated to define the linkage between informational and operational risk.
7. Recommendations 7 and 9 will be coupled; Recommendation 8 will be modified to call for risk assessment routines to be put into private and public sector supply chains in standard terms.
8. Recommendations 10 and 11 are removed as Project Endurance should cover the call for consistency in Government messages to industry on security, and there are other initiatives elsewhere. Recommendation 12 will be modified in consultation with APACS in the light of recent developments. A new recommendation was proposed for an annual prize for the software vendor who provided guidance most effectively using plain English.
9. Recommendation 13 is retained and Recommendations 14-16 combined. Recommendation 19 is rejected, and Recommendations 17 and 18 replaced by a statement; the need is now to raise awareness of the security tools available.

1. Introduction

1.1 This meeting was a sequel to the EURIM-IPPR E-Crime Study meeting in February which had led to the working paper 'Partnership Policing for the Information Society – Reducing Opportunities for E-Crime' drafted by Chris Sundt.

1.2 The aim of the meeting was to review the recommendations in the working paper, in the light of recent developments.

1.3 The current set of e-Crime meetings afforded an opportunity to update the work done so far, and should lead to the publication of discussion papers and recommendations by October or November. The forthcoming series of industry events on Information Security will provide platforms to put the recommendations onto the political agenda, and into the manifestos of the main political parties. In early February 2005, we plan to hold a major event with IPPR, with a ministerial response. Some recommendations had already been accepted, and if the timetable was met, ministers can be expected to respond

2. Comments and discussion of paper

2.1 The working paper considered reducing opportunities for e-crime in a number of different ways:

- education and awareness;
- managing risk and building trust;
- looking at commercial opportunities;
- looking at technical solutions.

2.2 Security should be promoted through the supply chain, with adherence to three principles:

1. security should be easier than insecurity;
2. security should be cheaper than insecurity;
3. security should be a community issue.

2.3 It was agreed to 'park' the first six recommendations on education and awareness because these issues were largely addressed by Project Endurance, which is essentially a drive by Government and Industry to coordinate public and SME awareness on the importance of security, and what needs to be done. They were also published in the discussion paper "Protecting the Vulnerable".

2.4 A 'good housekeeping approach' was preferable to one in which measures were concentrated on countering moves by 'the bad guy'. The approach using the 'three principles' (s. 2.2) afforded a means of ensuring that security was approached from the perspective of prevention rather than cure. These issues are also considered in detail in the revised 'Skills for Justice' paper.

2.5 Risk assessment is easy to say, but difficult to do, because very few people fully understood what was meant by the term. Although it is an implicit theme within managing risk and building trust, we need a specific recommendation on the importance of risk assessment, as this was rarely done well, even by the banks. The British Standards Institute has a working group that is looking at writing a Part 3 of BS7799 on risk assessment – this could be tied in with the recommendation. (This is a code of practice for information security management systems that has been a standard since December 2000, and can be used for compliance, but because there are no auditable standards, companies cannot be certified against it).

2.6 A spin-off from the EURIM Personal Identity Group meetings has been a discussion on the desirability of running an exercise in the practical application of risk assessment techniques. This has implications for liability issues (e.g. how computer systems change liability, or how corporations can avoid liability).

2.7 There are concerns about BS 7799 because of the way it is applied; we need to raise people's awareness of the risks, and a simple model, perhaps made available through the DTI Business Link, is needed. We need to raise the profile of risk assessment. Perhaps risk is defined best as a measure of uncertainty of outcome: risk assessment involves identifying threats, critical business assets and their vulnerabilities, and looking at their relationships. Managers need to have the competence to identify threats and undertake risk assessment objectively.

2.8 A recommendation on who should be looking at these issues was needed. The CBI may be a suitable vehicle: CBI has proposed the production of a business guide aimed at SMEs, asking whether they were secure or vulnerable in their supply chain, how they could identify risk and what they should be doing about it. This had received a very positive response, and CBI was developing content for the guidance now in plain English, with risk assessment as a key part of it. CBI planned to hold regional workshops to help SMEs, not relying on leaflets but reaching out physically to all firms.

2.9 The IT field is one of rapid and continual change, increasing vulnerability and making risk assessment increasingly difficult. A proactive approach to system security and risk assessment, with proper evaluation of assets, would reduce the problem of rapid change. However, a significant problem was a lack of knowledge, ownership and prioritisation of the assets a company held. Companies may only react once they have been attacked! There is thus a need for long term continuity in applying measures, an issue being addressed by the Jericho Group.

2.10 There is a need to ensure that risk assessment is part of the specification of skills sets etc. A solid recommendation should therefore be that the relevant professional bodies should be working with the Sector Skill Councils to include risk assessment in the skills sets being and training programmes. Though non-mandatory, the SSC would be tasked to implement the recommendation.

2.11 According to the Turnbull report, a risk present in a company must be effectively managed to reduce it and mitigate subsequent liability and/or damage; liability is incurred and insurance rendered invalid if assets are unprotected; a recommendation to strengthen the Turnbull recommendations to include an explicit statement requiring corporate governance obligations for information assets and risk assessment would be helpful.

2.12 The driver for security awareness in the USA is compliance, but not so in the UK. However, compliance would not achieve security if the aim were wrong; we needed a more intelligent approach. If BS7799 Part 3 included prioritisation of the objectives of Part 1, we could see a functional sequence of actions with risk assessment at the top. Unfortunately, there is a tendency today to react to security problems, when having a policy is prerequisite to risk evaluation. The first task of a training programme should be to determine the objectives and how to achieve them: the appropriate technology to support the policy can then be bought.

2.13 The following requirements were proposed for inclusion in recommendations:

- the professions to work with sector skills councils to produce specifications;
- standards of competence to be required;
- the need for the various regulatory bodies to require information assurance in corporate policies (CSIA had talked about extending an information assurance requirement to SMEs). There was also a need for the application of similar disciplines in the public sector.

2.14 A 'one size fits all' approach, which could be dangerous. It is preferable to equip people to protect themselves and avoid putting trust in systems that they do not understand; this would be achieved by referring to appropriate standards and routines (plural).

2.15 The relationship between corporate governance and information assurance is unclear. A point of leverage would be to make risk mitigation strategies part of the contractual terms of all links in the supply chain. Additionally, the Turnbull report should be updated to define the linkage between informational risk and operational risk, and to make clear that without information security, there could be no operational business. This amounts to an additional recommendation – and we need to identify who should implement it. We could then contact them and discuss how it might be done, thereby applying some pressure. **A key action from the meeting would be to approach members of the Jericho Group, to see if anyone would take this up.**

2.16 Government action in this area, and in its own supply chain, could be the basis for another recommendation!

2.17 Data sharing initiatives within Government should address the issues of mutual insurance, data sharing and risk assessment, in a similar way to that in which the private sector is now doing. This places the remit not with CSIA, but with the DCA and into the Gershon efficiency agenda, where the

objective is to remove obstacles to data sharing. It should also be a task for the new CIO to ensure that Governmental–departmental-supplier networks are secure: this could be an opportunity to change the emphasis from data protection to data sharing.

2.18 There is a perception that Government considers all those outside the 'GSI' field as insecure; this attitude needs to be changed before there can be an effective change in policy.

2.19 Recommendation 8 will be modified to call for risk assessment routines to be put into private and public sector supply chains in standard terms. Recommendations 7 and 9, dealing with the production of guidance and the channel employed respectively, should be coupled.

2.20 Project Endurance could to some extent cover the call for consistency in the message Government gives to industry in Recommendation 10, particularly with respect to security and the promotion of broadband. This could include a call to ensure that Project Endurance receives cross-cutting support from Government departments, notwithstanding the various pressures operating within Whitehall.

2.21 With regard to Recommendation 11, EURIM would be undertaking a separate review of reporting structures. ISPs have the capacity to do more in terms of systematic tracking and tracing in collaboration with law enforcement agencies. Recommendation 11 should be rejected as it does not task any body specifically, and there were other initiatives elsewhere. The community concept is to encourage people to work together to protect information assets.

2.22 There could be value in having an additional recommendation that there be a well-publicised annual prize for the software vendor who provided guidance most effectively using plain English! We should pass this to Computing and Computer Weekly to run the competition (with a warning to beware similarities with phishing attacks).

2.23 Recommendation 12 will be updated in consultation with APACS, in the light of work done with credit card companies (and APACS); more now needs to be done to remove obstacles to more effective vetting.

2.24 Recommendation 13 was intended to refer to the provision of guidance that SMEs can use with confidence, such as 'GIPSI' (General Information Assurance Products and Services Initiative) led by CESA and CSIA. The group works on defining and promoting UK pan-governmental requirements for information assurance products as well as establishing the means to ensure that those requirements are met (a kind of security kite mark process). Some kind of business model is needed for security health checks, which retailers will promote and sell at the same time as the system – thereby making money while solving the problem by selling secure systems.

2.25 An annual security check should be introduced to raise security issues directly with SMEs – thereby demanding attention and a human response so that the user understands what they are doing. The education process is necessary to justify renewal, while maintaining an online updating service.

2.26 Recommendations 14-16 are to be brought together. It was noted that while a qualification is soon out of date, a licence requires qualifications to be updated, e.g. through continual professional development. This can be incorporated in the new recommendation.

2.27 Recommendations 17 and 18 are to be reduced to a statement, and Recommendation 19 is rejected. There is now a need to raise awareness of what tools are available, because the market is already providing many of the tools, together with comprehensive guidance.

3. Conclusion

3.1 The meeting closed at 1200.