Review of the OECD Security Guidelines

Initial Comments to the Expert Group

Roger Clarke
Roger.Clarke@xamax.com.au
26 March 2013

0. Background

My comments are based on several decades of experience in eBusiness and eGovernment consultancy, academic research in relevant areas, and public interest advocacy work in consumer rights and privacy matters.

I have only very recently joined the Group, and am providing my reactions to Discussion Papers A and B, version 1.0 dated 8 February 2013.

There are many aspects of the two papers that I substantially support. These include:

- the aim of sufficient generality to remain relevant through a 5-10 year timeframe, across diverse cultures, styles, and stages of economic and social development
- the intention that messages be expressed at a moderately high level of abstraction
- the avoidance of the national security, cybercrime and cyberwarfare memes
- the avoidance of IT jargon – provided that such technical aspects as are relevant to a sufficiently deep understanding of the topic are included, expressed in an understandable form
- the focus on risk assessment and risk management, rather than the mirage of absolute security
- the strong support for openness, while recognising the need for balance, and justified forms of closedness as well as openness
- the explicit recognition that economic and social inhibitions arise from many security safeguards, especially where an excessively closed approach to security is adopted
- the inclusion of the holistic and cyclic notions

The remainder of these comments focus on aspects where I suggest that a somewhat different approach should be taken.

1. The Security Model

The conventional model (referred to in part in Document B on pp. 2, 3 and 7) can be summarised as:

Threats impinge on Vulnerabilities
resulting in Harm to Assets

It appears to me to be essential that the document make clear, at an early stage, the scope of the Assets under consideration. All discussions are affected by this decision, and considerable confusion will result if discussants are implicitly assuming different scope-definitions.

2. The Scope of the Assets

Document B on p. 4 characterises the previous iterations of the document as having been concerned respectively with 'siloed and isolated' IS and 'siloed and interconnected' IS. Those made good sense at the time; but I agree that a new orientation needs to be adopted for the current version.

From the Documents, a natural way of defining the scope of the 2013 document appears to be:

'IT Infrastructure Supporting the Digital Economy and Society'

The desire to avoid an excessively technical orientation is sensible. On the other hand, it would not be appropriate to define the Asset as, say, 'The Sources of Economic and Social Prosperity'. An excessively broad scope of that kind would encourage vagueness, and collide with other groups that consider economic and social policy to be their domain rather than that of the Security Expert Group. The solution I suggest is to define the Asset as being IT Infrastructure, but with a qualifying phrase that places the technical aspects firmly within the intended economic and social context.

The term 'Economy' by itself would be too narrow. Including the term 'Society' reflects the substantial use of IT for purposes other than commerce. It is consistent with the OECD's recognition that its members and their citizens are concerned about social as well as economic considerations.

The term 'Internet Economy and Society' is tenable. However it is limiting. The current technologies are aging, and there are increasing endeavours by governments and corporations to significantly alter the Internet's nature and governance. It is inevitable that some degree of fragmentation, of renewal and of replacement, will all occur during the 5-10 year planning horizon suggested in Document A on p. 2.

I accordingly suggest the constructively vague term 'Digital Economy and Society'. If the 2008 Seoul Declaration makes it necessary or politic to use the term 'Internet', then I suggest that the text make clear that it refers to 'inter-networking arrangements' rather than being necessarily limited to the TCP/IP based Internet of the 1983-2013 era.

I've suggested the term 'IT Infrastructure', although 'ICT Infrastructure' would serve equally well. By this I mean the devices, software and networking facilities over which services are delivered. The term's scope is suitably flexible. It may refer only to the lower layers of the architecture (e.g. in discussions about deep packet inspection performed in intermediating nodes on backbone networks, and the embedment of rootkits in consumers' devices), or to only the higher layers (as in discussions of P2P's potentials, threats and vulnerabilities), or to all-layer / end-to-end security designs (such as Virtual Private Networks). It can also, in any given context, be defined to encompass specific services (such as Internet Banking), or to extend only as far as the components on which a service (such as Internet Banking) depends and leverages.

3. Levels of Abstraction, and Perspectives

The documents, both implicitly throughout, and explicitly in Document A, pp. 2-3, select Levels 2 and 3 (Strategic and Functional) in preference to Levels 1 (Mission and Values) and 4 (Operational).

I perceive two serious problems, both arising from the embedded assumption that the levels are to be defined solely in terms of "governments and organisations", and that conventional institutions such as 'senior decision makers', 'directors', 'heads of line management', 'heads of ministries' and 'policies and procedures' are a sufficient basis for discussion.

(1) Hierarchies versus Networks

The current formulation of the levels of abstraction is presented in terms consistent with command-and-control mechanisms, or strictly hierarchical forms of governance.

There are many contexts in which such models are inappropriate. Examples include industry sectors (such as banking and airlines) and supply chains (which focus on the multi-corporation production-line rather than on the functions). The hierarchical view is even less applicable in the case of highly internationalised or globalised sectors and chains.

In the social arena, meanwhile, societies and communities are much better modelled using networks than hierarchies, even where transaction costs are not a motivating factor. As with economic networks, social networks also transcend nation-states, and challenge excessively structured command-and-control notions. Moreover, purely hierarchical thinking is antithetical to the notion of democracy. Even in its most simplistic form – a representative democracy with lengthy parliamentary terms – a strong feedback loop exists in the form of the ballot box.

(2) Authoritarianism versus Participation

The limitation to a hierarchical model and the exclusion of networks brings with it a strong emphasis on the formation of policies at each Level by an elite that operates in isolation ('policy makers develop policy'). This problem is exacerbated by the proposition that there should be "a common security approach for all" (p. 3).

The discussion of 'participants' and 'stakeholders' in Document B on p. 6 needs to appear much earlier, and to culminate in a positive statement about participative processes, inclusiveness, and a multi-perspective approach to the topic.

I therefore believe it is essential that the segments on Levels be re-worked, firstly to encompass both hierarchical and network architectural models, and secondly to expressly recognise the role of public transparency, consultation and participation in the evolution of policy.

4. Openness

In Document B on p. 2, one Message is expressed as 'Openness of the environment'.

I strongly support the notion, but the section would benefit from further articulation in order to connect with other discourses, such as:

- open source software, particularly its transparency to 'many eyes', and hence the greater likelihood of 'white-hatted eyes' detecting vulnerabilities as quickly as 'black-hatted eyes'
- open content, particularly the vital importance of reducing the dead weight of excessive patent and copyright monopolies
- communications inter-operability, particularly the open protocols necessary to enable reliable inter-connection and the avoidance of proprietary protocols with their inherent dependence on secrecy in an attempt to avoid exploitation of their vulnerabilities
- content inter-operability, particularly the open format standards necessary to ensure compatibility, and avoid obscurity-based monopolies and their inefficiencies and insecurities