

SECURITY BY DESIGN SUB-GROUP

SUMMARY

October 2010



Can society afford to rely on security by afterthought not design?

Society is increasingly reliant on complex online systems and vulnerable to online risks and threats. Many reports and recommendations have been made for retrofitting privacy and security to existing systems. ISA (EURIM) has summarised in a 4 page paper (www.eurim.org.uk/activities/ig/1010-SbD_4page.pdf) why this approach will fail, because security must be built into systems from the start. Links are provided to a more detailed report and sources.

The key points are:

1. Security has to be built in from the start and from the top

New online business models, including cloud computing, present risk-management challenges that cannot be resolved by retrofitting security. Government's most important role is to change market behaviour by ensuring security is included in the initial design and subsequent procurement of its own systems and services. Clear statements of the level and nature of security expected should form part of the initial planning for all public sector programmes, with the techniques to audit the required integrity, reliability and resilience included in the subsequent procurement specification.

2. Common terminologies and shared processes are critical to success

Government should support the provision of shared audit services and databases of assessed products and services and help enable these services to be widely used at affordable cost: perhaps building on the work of the National Technical Authority for Information Assurance (CESG) and the Centre for the Protection of National Infrastructure (CPNI).

3. Policies must be linked to processes for turning principles into practice

- The relevant professional bodies should review the standards of competence and integrity they expect of their members and co-operate to improve the quality of registers of current practitioners and reduce duplication of effort and cost.
- The relevant trade associations should facilitate co-operation in validating and cross-licensing audit tools and techniques so that these are routinely used, including by small innovative firms, while fairly rewarding those who develop and maintain them.
- Accounting, actuarial and legal professional bodies should work with those for information and security and technology systems to produce shared practice notes and guidelines on assessing the value and security of systems. The aim should be to help support better-informed decisions on investment, liability, responsibility and insurance.
- Government, Industry, professional bodies and education and training providers (including those responsible for electronic warfare, law enforcement and service delivery) should co-operate in bringing the current confusion of relevant standards, accreditations, qualifications and courses into line and fit for purpose.
- The Law Society should be asked to convene a cross-professional group to look at whether mass market systems without embedded SbyD are "fit for purpose" and to draft guidance for members who may be consulted on the consequences that might arise from legal action in this area.