

Security by Design Sub-Group

4 page summary of a 14 page report:
www.eurim.org.uk/activities/ig/1010-SbD_Full.pdf

October 2010:

The Information
Society Alliance

EURIM



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

The online world is increasingly vulnerable to accident let alone attack

Modern society is reliant on complex online systems whose ability to survive fire, flood and finger trouble¹, let alone fraud and attack by foreign powers, is uncertain. Meanwhile the cost of deliberate attack, including fraud, is rising sharply. Many reports recommend retrofitting privacy and security. It is much cheaper and easier to build this in at the design stage and if we wish the next generation systems to be more secure we have to start now, making positive use of the current moratorium and review of publicly funded systems to build on the best of private sector practice.

Meanwhile, convergence, increased system complexity and the transition towards new online business models, such as cloud computing, present risk-management challenges that **cannot** be resolved by security provided as an afterthought. Action is also urgently needed at service, system and product levels to reduce the rapidly increasing threats from criminals, terrorists and cyber-warfare to the systems on which society depends.

The key is to change market behaviour

Government, regulators and professional bodies have important roles but government's main contribution should be as a more intelligent customer. The UK Government, its security advisors and the leading providers of ICT services must work together to agree common terminologies and shared processes for practical co-operation. They should focus on frameworks for assessment and audit, make it very much cheaper and easier to follow good practice, build on and replicate what works and is known to be secure. Unless they do so we will become ever more reliant on offshore products and services of unknown provenance.

The formation of security policies by government and regulators should not only involve the relevant trade associations and professional and academic bodies but also be peer reviewed by current practitioners, both public and private sector, including those with responsibility for delivery, operations and monitoring. They should be designed to support and reinforce good business practice that makes the UK a location of choice for trusted, globally competitive online services.

Key Recommendations

1. Clear statements of the level and nature of security expected should form part of the initial planning for public sector programmes, with the techniques to audit the required integrity, reliability and resilience included in the subsequent procurement specification.
2. 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:

¹ It is widely believed, although we can find no substantive evidence, that operator error, including during routine maintenance, has brought down many more systems, both public and private, than hostile action.

perhaps building on the work of The National Technical Authority for Information Assurance (CESG) and Centre for the Protection of National Infrastructure (CPNI).

3. Professional bodies, such as The British Computer Society (BCS) and the Institution of Engineering and Technology (IET) and the UK chapters of the international associations, 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.
4. Trade associations should facilitate co-operation in the validation, cross-licensing and use of relevant audit tools and techniques so that these can be routinely used, including by small innovative firms, while fairly rewarding those who develop and maintain them.
5. 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 to support better informed decisions on investment, insurance, responsibility and liability.
6. 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 standards, accreditations, qualifications and courses into line and fit for purpose.
7. 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.

Changing Market Behaviour

The Internet does not have in-built security. Until recently those responsible for planning and procuring online systems have usually focussed on facilities, cost and ease of use. Resilience and security have been after-thoughts, often leading to a reactive approach to threats, patching vulnerabilities when discovered.

Risk capital is hard to come by during or after recession. Major procurements are driven by the public sector and those leading private sector players who can afford to invest for the longer term. The insurance industry has a key role in setting standards but requires credible, cost-effective routines to assess the effect these have on the risks they are being asked to cover before they can afford to offer lower premiums.

The main obstacle to tapping the latent demand created by customer fears is not the lack of certification routines but a lack of common, credible, cost-effective frameworks within which to use the routines that already exist. Such frameworks need sets of semi-automated, open source routines that buyers and suppliers can use and insurers will recognise. Small suppliers can be particularly effective in producing innovative components to plug gaps but are deterred by the overhead cost of multiple, overlapping certifications and accreditations.

Regulation and legislation can change market behaviour but the rate of change in the market place often renders legal or regulatory initiatives obsolete before they are operational. A good example of an Industry response is the IdenTrust frameworks created by the banks to provide efficient and effective international and intra-national cross-sector, contract-based, "self-regulation".

Central Government should ensure that security is not treated as an "add-on" to planning and procurement. Consideration of the need for security and resilience should be embedded in initial policy proposals.

Proposals for change need support from bodies such as the Royal Academy of Engineering, BCS and IET in the UK, the Institute of Electrical and Electronics Engineers (IEEE) in the United States and Information Systems Audit and Control Association (ISACA) and the International Information Systems Security Certification Consortium (ISC), to establish professional credibility.

Culture change in the public sector will entail mandatory requirements from OGC, Audit Commission and NAO – not just “policy” from CESG and Cabinet Office. Culture change in the private sector entails providing finance and marketing directors, auditors and company secretaries with convincing material on the value of investment in improved information quality and network and system security, information and the need to treat it as an “asset” to be valued and invested in. Hence the importance of the work of the ISA (EURIM) group on the “Value of Information.”²

The biggest challenge is not the scale of the investment needed for change. Much of this has already been made by major defence suppliers. It is to make the business case for pooling that effort. Boards need to be convinced that they will profit more from selling robust products to larger and better educated markets, than from patching threats in response to law suits and regulatory interventions.

The Case for Security by Design

Security not performed by design is currently dependent on pockets of good practice among companies who understand the business rationale. SbyD at the product level is a beginning not an end, but it is an essential beginning to building secure and resilient systems and networks and to delivering secure and reliable services over them. ICT systems serving the public do not become secure and resilient just because a few “good citizens” act in a responsible manner. A wholesale transformation where SbyD is the norm requires compelling forces to make markets respond.

Governments around the world are increasingly aware that national infrastructures are heavily interdependent on ICT systems that are intrinsically at risk and cannot be protected solely by legions of firewalls, intrusion detection and prevention systems. The case of Gary McKinnon, who is facing extradition to the United States on charges of perpetrating what one US prosecutor claims is the “biggest military computer hack of all time”³ illustrates the damage that can be done by a single individual supposedly looking for information on UFOs.

As public services begin to use cloud computing services that transcend national boundaries, critical infrastructures will become inter-dependent across international boundaries. This raises privacy and security challenges where regulatory and legal claims need to be enforceable across jurisdictions.

The transformation of ICT systems from separate to converged technologies, from LAN-based to cloud computing, is already happening. The UK is no exception. There can be no assurance that critical ICT systems will be made secure without the necessary steps being taken to require that systems and services be certified to internationally recognised (if not necessarily formally agreed) industry standards to establish and maintain a high level of trust.

As in any complex system, the security of ICT involves the interplay of technology, people and processes. With respect to the design of the technology it requires that the ICT industry takes its own transformational steps starting with a transition to Security by Design.

Models already exist that can guide the process. ITU/T X.805 provides a framework for assessing the security of complex networked systems that involve components of many types, from many sources. The ISO 27000 series is well known and widely used for specifying, documenting and auditing secure processes. The Kantara Initiative is one of many for identity management systems. The main ICT and security professional bodies are engaged in similar exercises around the world.

² “From toxic liability to strategic asset: unlocking the value of information”

http://www.eurim.org.uk/activities/ig/0911-Value_Summary.pdf

³ Boyd, Clark (30 July 2008). "Profile: Gary McKinnon". BBC News.

<http://news.bbc.co.uk/2/hi/technology/4715612.stm>

How to Begin

The first steps towards Security by Design must come from industry and government together taking a shared end to end systems approach, creating market motivation, on both sides, to invest in SbyD during the initial design stage, leading through integrated service delivery. There must be consequences for non-compliance to new standards – including for those who fail to take it into account during the pre-procurement phase for new public sector systems.

In the short term there is a need to establish a clear and well-defined terminology. Terms such as “cyber security”, “information assurance” and “federated identity”, all suffer from multiple meanings.

A major stumbling block is the failure to share information on threats and problems. Many government agencies do not share because of “state security”. Suppliers are reluctant to share that which they believe will give them business advantage. Private sector users are similarly reluctant to share that which might jeopardise customer confidence. Removing the roadblocks to information sharing requires establishing tamper resistant, trusted mechanisms for the confidential reporting, collection and analysis of that which will help address common problems.

Whilst a focus on security at the architectural level provides the necessary top down structure, a parallel, bottom up, approach is also needed to ensure products are developed to known security baselines. There is a need for clearly defined, comprehensive governance models that support both security processes and technologies. Adequate system-level policies are also needed within SbyD frameworks. These should drive the requirements for security.

In the longer term common systems level approaches to the implementation of SbyD are fundamental for secure system development. Clear/transparent audit trails of “who did what and when”, in any transaction, are fundamental in an online world. Accountability, with clear entitlements and obligations (which vary from one application to another), are integral to trusted solutions.

The public sector has much to learn from the “minimum operating requirements” used in private sector applications (e.g. financial services and payment systems) where a high degree of reliance and security is integral for daily operations and any mandatory policy must be based on sound professional principles and practice, beginning with clear statements of the level and nature of security, reliability, resilience and integrity expected. To be effective it also needs the creation of an infrastructure for re-usable third party audits to greatly reduce duplication of effort and cost. That will require working with trade associations on the issues of cross-licensing.

There is also a need for government, as a major employer, to work with professional bodies and education and training providers to bring standards, accreditations, qualifications and education into line with what is needed and to ensure management understanding. That needs to include a common recognition, at all levels from policy to day-to-day operations, that people processes are more important than technology. In particular, complex systems for mass-market use should be supplied with default settings for secure and average use, with clear guidance to customers on how to change them and what their responsibilities are.

The HMG Security Policy Framework⁴ is an important part of the policy but is only a part. Creating the market conditions conducive to “Security by Design” is also just a starting point. Beyond this, progress will only be made in cooperation with the customers, large and small, who make the markets work.

⁴ <http://www.cabinetoffice.gov.uk/spf.aspx>