CAN SOCIETY AFFORD TO RELY ON SECURITY BY AFTERTHOUGHT NOT DESIGN?

Status report and recommendations of the ISA (EURIM) Subgroup on Security by Design

October 2010

OBJECTIVES

This report makes the case for a fundamental change in market behaviour so that the complex IT systems, on which society increasingly depends, have security embedded from the start rather than added as an afterthought.

The report was produced by a working group chaired by Carlos Solari (CIO of The White House 2002-05, now with CSC). The vice-chairmen of the sub-groups included John Bullard (IdenTrust), Richard Goodall (EADS) and Paul Wilson (DeLaRue). The contributors and reviewers included representatives from Alcatel-Lucent, BCS, EADS, Fujitsu, IBM, IET, IISP, ISACA, ISC^2, ISSA, Jericho Forum, Logica and UK Payments. The drafts were circulated to observers, including those in the Cabinet Office, CESG, CPNI and OGC.

CONTENTS

CAN SOCIETY AFFORD TO RELY ON SECURITY BY AFTERTHOUGHT NOT DESIGN?

"The main benefit of investing in better security technology is to force the enemy to concentrate on corrupting your people instead of trying to break your systems."

Professor Richard Walton, former Director, CESG

Executive Summary

1. The Current State of Cyber-security

Society is increasingly reliant on complex online systems and vulnerable to online risks and threats. Many reports recommend retrofitting privacy and security, but much more needs to be done to ensure it is built in at the design stage.

2. Changing Market Behaviour

Government, regulators and professional bodies have important roles but the key to changing market behaviour is better practice in design and procurement. Government's main contribution should be as a more intelligent customer.

3. The Case for Security by Design (SbyD) and by Default

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 threats from criminals, terrorists and cyber-warfare to the systems on which society depends.

4. How to Begin

The UK Government, its security advisors and the providers of ICT services must play a leading role in agreeing common approaches that will change market behaviour. These must include common terminologies and shared processes for practical co-operation, focusing on frameworks for assessment and audit.

5. Policies must be based on Sound Professional Principles and Practice

The formation of government and regulatory policies should not only involve the relevant trade associations and professional and academic bodies but should also be peer reviewed by practitioners, both public and private sector, including those with responsibility for delivery, operations and monitoring.

Key Recommendations

- 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.

- 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 Centre for the Protection of National Infrastructure (CPNI).

- 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.

- 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.

- 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.

- 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.

- 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.

1 The Current State of Cyber-security

1.1 Government data handling – a salutary lesson

New threats to public and private sector information networks are discovered nearly every day, while inadequate security and information losses have inflicted unacceptable damage to confidence and trust in the Government's ability to safeguard our data. Politicians and senior civil servants need to know what these threats are, and why the current 'security by afterthought' measures are failing.

The loss of IT hardware by the British Ministry of Defence (MoD) and the loss of removable data storage media by HM Revenue and Customs (HMRC), both involving large volumes of personal data, were among the most high profile of what seemed to be a slew of such incidents. Reports of data handling procedures were commissioned (for example, the Coleman[i], Poynter[ii] and Burton[iii] reports).

The National Information Assurance Strategy[iv] of 2007 and the Hannigan Review[v] of June 2008 demonstrated that the government was moving from a purely reactive stance to the formulation of a cross-governmental strategy designed to pre-empt such incidents by means of a set of standard behaviours and processes applicable across Whitehall departments.

The common themes emerging from these reports could form the foundation (along with ISO 27001 and the Government's Information Assurance Maturity Model[vi]) for shared standards for information assurance across both public and private sectors.

There is, however, little evidence that the public sector has drawn on private sector experience in this area, particularly with regard to critical systems in, for example, financial services. The very different approaches of public and private sectors to risk management, as well as to responsibility for action and liability for the consequences, can get in the way of practical co-operation. This may therefore mean that serious progress will only be possible after even more serious incidents.

The Information Society Alliance (EURIM) recommends that action should be taken now to set out standards for IT Security based on the premise that embedded security is a fundamental principle of the design of any system supplied to the UK Public Sector and that those formulating standards draw on private sector user, not just supplier, experience.

1.2 Falling confidence and a rising tide of fraud, extortion and cyber-attacks

Society at every level is increasingly dependent on the reliability and availability of online services, with much debate on preventing data loss and improving protection against outside attack. Most corporate risk assessments give a higher probability of serious damage resulting from design or operational error or from inside attack, rather than outside attack.

Despite this, reported losses from online/computer-assisted theft and fraud have risen sharply, with major incidents combining insider activity with external attack. Card-holder not-present-fraud loss reported to the UK Payments Council increased by 13% from £290.5 million to £328.4 million in 2008 and now accounts for 54% of all card fraud losses.[vii] Losses from online banking fraud increased by 132% between 2007 and 2008 with losses totalling £52.5 million in 2008.This sharp increase can be attributed, in part, to the 43,991 phishing websites targeting UK banks and building societies in 2008, up 171% from 2007. Phishing sites are becoming more prevalent and increasingly sophisticated, including those used for attacks on Government online services, wherever these are hosted. Organised crime has geared up to exploit long-standing weakness in credit card and direct debit mechanisms and their linkages to other online payment services[viii]. To these should be added losses recharged to business or written off as bad debt. According to the Federation of Small Businesses (FSB)[ix] recharged losses are under £5,000 in two thirds of cases, but given that most FSB members have a turnover of under £100,000, it is unsurprising that so many small firms are unwilling to transact online.

A growing number of customer/client databases (both public and private sector) are falling into criminal hands as a result of insider fraud, external attack or opportunistic data "acquisition". This is expected to increase as companies layoff staff or sell surplus equipment without removing stored data. Governance processes are likely to lose rigour following a merger or acquisition or to lapse entirely if an organisation is placed in administration.

The profitability of communications and online service providers and retailers has fallen. This impacts on the ability and desire to reimburse theft or fraud to retain consumer confidence. Only 13% of respondents to the FSB survey[x] were implementing the Payment Card Initiative Data Security Standard while most felt this did not meet their needs, with compliance costs (including security overheads for those without in-house ICT, let alone security, expertise) higher than the value of the service in attracting business. There are also reports of consumers/small businesses being expected to cover the cost of fraud and/or having more problems obtaining redress. For example 29% of the FSB respondents had been a victim of card not present fraud, and 22% had had it charged back to them.

Meanwhile, while consumer surveys indicate that nearly half the public now depends on their broadband connection, more expect to be victims of online crime than of theft from their home or car[xi].

A recent survey conducted by the University of Chicago on behalf of Internet registry agency ICANN (the Internet Corporation for Assigned Names and Numbers) found that more than 75% of Internet domain registrants have incomplete, invalid or false names, while 22% of website owners proved to be impossible to trace[xii].

Large-scale content piracy, plagiarism, impersonation and theft have caused ICANN and some national registrars (such as Nominet in the UK) to take serious steps to improve the security and governance of the domain name system.

The success of cyber-attacks on small countries (e.g. Estonia, Kyrgyzstan), government agencies (e.g. US State Department) and major service providers has revealed the scale and nature of current vulnerabilities to deliberate attack. Financial services, online gaming and retail users are losing billions from computer assisted fraud and extortion and are actively seeking more credible solutions.

Owners of Intellectual Property Rights increasingly expect "intermediaries" to help take action against customers engaged in the plagiarism of research or piracy of content or designs, as with routines for enforcing some of the provisions in the Digital Economy Act. Similarly, those suffering reputation loss as a result of impersonation or libel, whether corporate or personal, are also holding intermediaries to account if they do not help secure redress.

The public sector is being forced to integrate its networks to reduce cost while seeking to secure them against cyber-attack and the threat of service collapse and civic unrest. Whether the "enemy" is a foreign power, organised crime, accident or "Act of God" there is a growing pressure from well-informed customers (e.g. aerospace, financial services, petro-chemicals and online retailers) for information that will enable them and their insurers to assess systems, services and their dependencies and to make informed choices as to the level and nature of risk they are willing to accept or underwrite.

2 Changing Market Behaviour

2.1 A task for markets more than governments

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. Most systems can therefore be said to be secure by "after-thought" rather than by design.

The Internet may have a robust set of elegantly simple any-to-any addressing protocols at its heart but we access it over a patchwork quilt of products and services of uneven and often unknown security and reliability. Few suppliers know whether the hardware and software components used in their systems were produced using formal methods for specification, design and audit. Major businesses within the critical national infrastructure rarely know whether the standby facilities for their "resilient" networks pass through the same "single points of failure" or know the operational processes (from password routines to staff vetting) followed by those more than one or two links out along their outsourced supply chains.

The ability to offer informed choice between "cheap and cheerful" and "secure and reliable" products and services will entail the routine use, by both buyers and suppliers, of audit tools and frameworks to assess the provenance, security, reliability and resilience of components in complex systems. The resultant risk assessments should consider not only whether software modules were developed using formal methods but also the people processes for applications, the physical land-line routings, radio paths, life of the battery back-up for radio masts in local access networks, vulnerability to flood, storm or power failure and so on.

To some extent governments around the world are already leading this process as they overhaul their defence communications procurement methods for a world of cyber-warfare. The CESG Claims Tested Mark,[xiii] for example, allows suppliers to submit a statement of claims (usually related to security, functionality, compatibility etc.) to be assessed for relevance and then independently measured for accuracy by ISO 17025 certified laboratories. If the claims are substantiated then they can display a logo accordingly.

The problems that arise from having tens of millions of potentially insecure systems in the hands of end-users also need to be better addressed. That includes encouraging products to be shipped with security facilities enabled and providing better guidance and support for consumers, both before and after they encounter problems. If confidence is to be sustained, end-users need to know who can help them and that they will not be held liable for what they do not understand.

There is also a need to inform audiences, at all levels, that there are no absolutes. There are only tiers and rings of security and trust in the "always on except in a crisis" world of integrated (fixed and mobile) broadband. Given the growing lack of trust in e-mails and phone calls purporting to come from banks there is a suggestion that such messages and the web addresses for more detail should be included with bank statements and other credible paper-based correspondence.

2.2 The means of changing market behaviour

Fear of loss, liability, accountability and insurance cover

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. Examples of rapid payback from small scale incremental investment to cut direct losses, reduce legal liabilities and restore confidence on the part of consumers can, however, be used to reduce perceived investment risk. The insurance industry has a key role in setting standards but requires credible and 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 accordingly.

Changing buyer behaviour by shared "certification" and accreditation

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. For example, many UK Government Departments require assessments to be repeated because they do not recognise, or do not have access to, assessments carried out by other departments. This can apply to people (e.g. the CESG Listed Advisor Scheme - CLAS consultants), products (e.g. IT Health Check Service - CHECK and CESG Claims Tested Mark - CCTM) and services (e.g. for those who wish to share or exchange data with central government departments over Direct.Gov).

Legislation and Regulation

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. It is also important to ensure that regulation is technology neutral and does not impact the market's ability to develop innovative and competitive tools and solutions to address security issues as and when these emerge. It is better to remove the obstacles to change.

There is a strong view among both suppliers and customers that laws should apply equally online as off-line, including responsibilities and liabilities: thus electronic "Bills of Exchange" are treated the same as their paper-based equivalent and the "publication" of incorrect information online can be regarded as libel.

This approach raises many issues of practical interpretation. The House of Lords report on Personal Internet Safety recommended placing responsibility for ensuring that products and services are fit for purpose on those who wish their customers to transact online[xiv].

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" - which national regulators would find difficult to emulate. The IdenTrust "contract" has become simpler, not more complex, over time as avoidable complexity is stripped out. This is the opposite to the behaviour pattern of most statutory regulators. There are similar, well-established, global, contract-based routines in Insurance and Freight Forwarding – e.g. Lloyd's Register and Den Norske Veritas.

Governments and regulators need to enable and encourage the providers of online services to develop similar internationally applicable routines – not to suggest or dictate what these should be.

Government as an Intelligent Customer

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. These should be reviewed as part of Gateway 0 and subsequently policed by the Office of Government Commerce (OGC), National Audit Office (NAO) (for Central Government) and the Audit Commission or its successor (for Local Government and Agencies). The way in which the US Office for Management and Budgets requires explicit reference to security in projects and links this to annual departmental cyber-security assessments is an approach which also merits consideration. CESG guidance and policies should, as far as practical, be published, reviewed, and understood by those they are supposed to protect. There are good reasons for "restricting" elements of compliance policy, including who needs to comply and their advisors, but the consequences of this need to be better understood by all concerned. This should help prevent situations like the much heralded system of individual learning accounts (ILAs), through which 2.5 million learners received credits worth up to £200 towards courses, which fell victim to abuse and fraud on "an industrial scale".

There is a need to pool expertise and share the effort of producing guidance and advice for next generation networks. Those involved, both centrally and locally, are seeking a transition to shared secure, reliable and resilient networks but lack the skills and tools to assess the products and services being offered to them. In consequence, proposals for sharing gather momentum and then collapse as problems emerge and confidence or funding evaporate (e.g. Ocean).

2.3 Creating trust: provenance, certification, accreditation, accountability

Trust is earned

Much effort has been spent trying to shorten the time it takes to earn trust in ICT products and services, particularly with regard to innovative products and services: e.g. the use of independently audited formal methods to verify components mathematically.

Most online services rely, however, on products and services from a wide variety of sources. Defined processes, such as X.805, are therefore also needed to establish the provenance of components in complex systems. Service delivery also depends on the behaviour, conduct and processes of those responsible for implementation and operation, including factors such as user training and the default settings in the systems they use for access.

Many systems have to make compromises between what is desirable and what is affordable and practical in operation and design. Trust in delivered security depends on more than just trust that the original design was suitable for the risks anticipated.

Frameworks for establishing Trust

The need for trust frameworks to be comprehensive does not change over time. They need to embrace hardware, software and network components as well as application "solutions" and service operations, using contractual frameworks such as IdenTrust and defined processes such as X.805 and ISO 27000 as well as formal methods such as Event-B, VDM, Z, and SPARK. Some of these may be "historic" but so is some of the code at the heart of the critical systems of today.

Such frameworks carry start-up costs but can lead to serious savings once established. Cutting the costs of these frameworks will enable routine use. But this will also necessitate the widespread use of automated tools to track the source and provenance of the components used; the operating processes of those in the supply chains involved and the geographic routings and physical dependencies of the transmission networks used. Such an approach also makes it much easier to enable claims of security to be independently checked – an essential step in building trust.

The dimensions of Trust

The dimensions of trust involve certification, accreditation and audit along supply chains serving different, but often overlapping, markets.

One dimension involves the "evidence" required by those (e.g. BT, Google, IBM, Vodafone or Verizon) bidding to supply networked services to knowledgeable customers (e.g. BP, HSBC or MoD) and involves their product and service suppliers (e.g. Alcatel Lucent, CISCO, De La Rue or EADS) and also the innovative small firms bidding to be component suppliers or specialist subcontractors.

Another dimension involves providing "evidence" to meet the different needs of those supplying low cost, advertising-funded services, those offering premium-rate services claiming to offer reliability, resilience and security and those wishing to make informed choices, whether as individuals or sole traders or as corporate or public sector buyers.

Generating trust depends to a large degree on establishing responsibility for the configuration of systems. It is not helped by proposals to pass liability to those who lack the information and understanding to make informed choices: e.g. removing the Internet access of those whose systems have been used without their knowledge for unauthorised file sharing. Complex systems for mass-market use should be supplied with default settings for either secure or average use, with clear guidance to customers on how to change them and what their responsibilities are.

Complex systems with Internet access are increasingly being embedded in a wide range of domestic and industrial products: e.g. smart meters, high definition televisions, computer printers and car maintenance diagnostic systems. There are allegations that some of these are now a point of vulnerability for attacking the networks to which they may be attached for maintenance or charging purposes. Guidance needs to include the consequences of enabling or disabling such access.

2.4 The points of leverage

Professional support is a pre-condition but not a sufficient condition

Proposals for change need support from well-respected national and international 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)[2], to establish professional credibility. Similar support is needed from relevant trade associations, such as Intellect, the UK Payments Council, bankers, defence contractors and insurers to establish industry support. But market change will ultimately depend on customer pressure from the top management of organisations that have serious purchasing power, including along their supply chains.

Bringing about public sector culture change from the top down

Culture change in the public sector will entail mandatory requirements from OGC, Audit Commission and NAO – not just "policy" from CESG and Cabinet Office. High impact events, such as 9/11, can bring about rapid culture change but data losses only confirm perceptions of public sector and corporate attitudes towards personal information. Change will usually only happen if driven by an event with an impact akin to that of 9/11 or by sustained political pressure. That pressure needs to be supported by well-informed, evidence-based guidance and impact analysis.

A key point of leverage is to brief the Class of 2010 – the largest new intake of MPs since 1945. Those not in office may well have equally important roles in Select Committees conducting pre-legislative scrutiny of proposals that are critically dependent on systems that are fit for purpose or monitoring subsequent performance. The plans of the Information Society Alliance (EURIM) to follow up on its well received guidance on good procurement practice are most relevant[xv].

Bringing about private sector culture change

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. This entails improved professional guidance on the direct and indirect value of good information and the need to treat it as an "asset" to be valued and invested in, as well as protected. Hence the importance of the work of the ISA (EURIM) group on the "Value of Information" and the recommendations in its report "From Toxic Liability to Strategic Asset: Unlocking the Value of Information."[xvi]

Removing the obstacles to change

The biggest challenge is not the scale of the investment needed for change: much of that investment has already been made by major defence suppliers in various parts of the world. It is to make the business case for pooling that effort, enabling and encouraging major suppliers to engage in open co-operation and fair trade, in the public interest. 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.

This also requires that governments, legislators and regulators do not prevent such co-operation, whether on grounds of "competition policy" or "national security". They need to accept that they are "local" players in global markets for secure products and services.

3 The Case for Security by Design (SbyD) and by Default

3.1 Growing complexity and risk

ICT is in the midst of a transformation, embodied in terms like cloud computing, network confluence and convergence. These changes should bring improvements in ease of access, the consolidation of physical infrastructures and the integration of content: voice – video – data. Simplification is one of the motivating factors. Separate infrastructures, each with different protocols, come together to share the same physical, highly distributed paths and logically come together to follow one set of protocols – not separate ones. In practice, this simplification is not at all simple. It requires new architectural,

engineering and design considerations that drive complex technology solutions with a new set of associated risks.

Convergence of the separate data infrastructures; voice and video all conforming to the Internet Protocol (IP) is presenting serious security challenges. Voice calls, for example, require different design considerations than those for email. Security must be re-thought and the complexity inherent in these changes must be part of that thinking. Many of these issues are being addressed internationally in the context of IPv6 – but few UK security groupings have the funding and resources to take part.

Currently, end users have primary responsibility to provide security by purchasing and installing security technologies (like firewalls) to protect their systems from outside attack. In 2007 the Jericho Forum[xvii], a consortium of major users in the banking, pharmaceutical and aerospace sectors, publicised the need for a new approach because many critical information systems and the information within them, were no longer contained within, or protected behind, the perimeter firewalls of the organisation.

De-perimeterisation

The term '*de-perimeterisation'* was introduced to explain the fact that the protection of information is as necessary *outside* the local area network perimeter as it is inside. Despite the move towards cloud computing, the security business model of perimeter-based thinking continues. De-perimeterisation places security at the heart of an organisation's distributed technology architecture, and is consistently implemented in end-user devices, application services, and critical information assets – where security will rarely be effective unless built-in from the outset.

Many have made the case that security is not something that can be applied as an afterthought: rather it must be applied at the points where the technology gets created, developed and brought to market, with full accountability:

> "Our computer managers have become accustomed to deploying systems with inherent weaknesses, buying add-on security solutions, and then entering a cycle of penetrate-and-patch. As new flaws are discovered, we deploy patches or else add on yet new security applications. There is insufficient effort devoted to really designing in security and robustness. This also has contributed to unprotected supply chains, where software and hardware developed and sold by entities is then placed in trusted operational environments: the (incorrect) expectation is that the add-on security will address the problems that may be present[xviii]".

3.2 Convergence means interconnected benefits but also interconnected risks

The implementation of IP-based systems has had repercussions for business and government. There is a long list of maladies infecting IP data systems and now convergence interconnects them by default. With IP systems converged with the telephone (VoIP) and broadcast video (IPTV), it is essential to consider that the threats will also "converge". The interconnections needed to integrate the technologies delivering the different mediums of information have inherent technical complexities. Poor security cannot be solved by add-on security applications. The dependence of Western societies on ICT demands that we ensure convergent systems address seriously the risk of misuse.

3.3 Security by Afterthought (SbyA) vs Security by Design (SbyD)

Without SbyD we have SbyA. Security not performed by design is at best dependent on pockets of good practice among those companies who understand the business rationale and have a sense of responsibility to work actively towards designing in security to their technology. 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. The post mortems into public sector systems security failures summarised in Section 1 provide ample evidence that SbyA is the current norm. The absence of discipline in the design stage of systems and technology development correlates with the cost of security breaches and the loss of trust in agencies or companies compromised.

3.4 Vulnerabilities abound

Left to chance (SbyA), vulnerabilities will increase not just in the individual product designs, but in the interconnections that make the technology work in operational environments. Convergent complexity then becomes the hackers' breeding ground where they can use unaddressed vulnerabilities to gain access.

Protected connections, data and system integrity are security requirements at product, network, and application levels. The Internet and all the web applications accessible over nodes across the world are not served by the technology of one company nor of one form of security. Security integration at the operational level, with different products typically from different companies, is where people and processes come together.

One of the most striking examples of this is identity management. Most Internet applications force some form of access control and authentication to identify end-users and establish the privileges of use. Unfortunately, in the absence of shared identity management systems, the need to authenticate each and every time for each of the thousands of services, leads rapidly to a complexity that is antithetical to the intended good practice of access control and authentication. This has been one of the compelling reasons for federated identity systems. This translates to the need for security by design at the service level, including addressing the issues surrounding shared identity management. These are being addressed in the new Identity Governance Group of the Information Society Alliance (EURIM)[xix].

3.5 Vulnerable infrastructures

Governments around the world are well 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. If the flaws are there on the inside to begin with, no amount of perimeter-based protection will do the job.

This is not theory but reality. 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,[xx]" illustrates the damage that can be done by a single hacker supposedly looking for information on UFOs. Planned investments in both the UK and in the US seek to apply ICT for a more efficient and resilient use of energy. The question is whether these investments will require SbyD or default to the idea that somehow security will happen by chance or can be added as an afterthought.

If cloud computing transcends national boundaries[xxi], then national infrastructures will become further inter-dependent between nations. This raises still further the security challenges where legal boundaries need to be enforced not just in physical but also in cyber dimensions. It becomes a matter of national security that these infrastructures continue to operate as intended and assured by the appropriate legal boundaries. This will not happen by chance - they will need to be secure by design.

3.6 No time to waste - but climb the mountain step by step

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 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 will require that the ICT industry takes its own transformational steps starting with a transition to SbyD. That requires beginning with the security of the components (building blocks or code or hardware), building these into secure structures (including hardware devices or applications software) in which the "system calls" to the components (to do what they were designed to do) are also secure and putting these together to deliver secure services operated by human beings who are not only themselves trustworthy but will also follow secure procedures.

Models already exist that can guide the process. The ITU/T X.805 standard provides guidance for the development of network security, and the ISO 27000 series standard guides secure system operation and how systems can be certified by independent auditors. The Kantara Initiative[xxii] is organised to

work out mechanisms for identity management. The main ICT and security professional bodies are engaged in similar exercises around the world.

Progress towards these aims requires the policies and motivations, from the top down, that will cause markets to change from accepting after-the-fact security (as in perimeter-based approaches) to rewarding those who design the security in their own systems and deliver security in the value chains to their customers. Only then will SbyD become standard practice.

4 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 to invest in SbyD during the initial design stage, leading through integrated service delivery. Resilience and standby capacity will be needed to counter the threats of cyber-crime and terrorism, (including "distributed denial of service" (DDOS) attacks using millions of compromised computers around the world) as well as those of storm, flood or fire and to ensure the continued operation of the nation's critical infrastructure.

There must be consequences for non-compliance to new standards and the issues must be discussed sooner rather than later because all the suggested solutions also have potential downsides.

In the Short Term:

4.1 Establish clear, well-defined terminology

Terms such as cyber-security, information assurance and federated identity, all suffer from multiple meanings. This adds to the confusion of an already complex situation. The first step is the development and use of a common language. All will benefit from this but we should not under-estimate the challenge to an industry mired in obfuscation, with jargon terms meaning different things to different audiences, let alone according to whether they are used by academics, practitioners or marketing men.

4.2 Increase dialogue and co-operation across government, security services and industry sectors

One of the big stumbling blocks to understanding the extent of the current threat is the lack of information sharing. Security services do not share because it is often restricted for reasons of state security. Suppliers are reluctant to share that which they believe will give them business advantage. Commercial users have to consider their reputation as a safe and secure institution with whom to do business. Thus a bank may wish to conceal the cost of cyber-attacks because the potential loss to business (a bank's business is trust) can far outweigh the actual losses incurred. Associations such as the Jericho Forum are beginning to make progress in providing safe information sharing environments, but such initiatives tend to be national/local in their perspectives. Removing the roadblocks to information sharing requires establishing tamper resistant, trusted mechanisms for the confidential reporting, collection and analysis of that which is necessary.

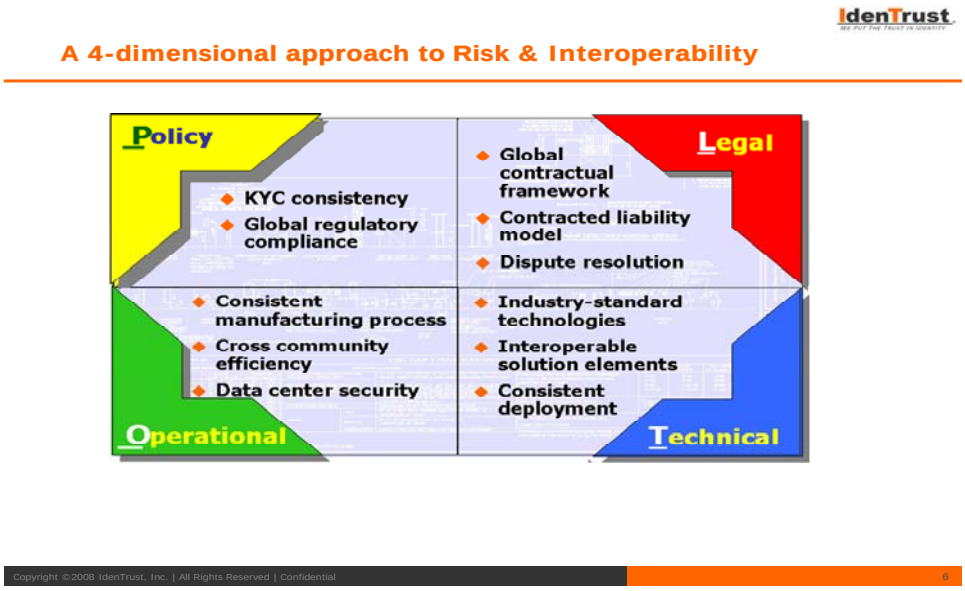
4.3 Focus at both the architectural and product level

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. New products need to be "proved" to have been designed with an SbyD approach that will fit within standards frameworks such as ITU/T X.805. There must also be mechanisms in place by which the major users agree which existing standards are to be used and built on in their common frameworks. The term "Policy Approval Authority" (PAA) is used for such mechanisms by, for example IdenTrust. Equally there must be routines for new standards to be introduced; to ensure the approach remains fit for purpose, current with evolving trends. These will be both technology and business driven changes.

4.4 Focus on a governance framework

A technical standard for the evaluation of ICT products to prove compliance is not sufficient to guarantee the security of a system. It is often the result of business or regulatory requirements rather than operational security needs. There is a need for a clearly defined, comprehensive governance model that supports both security processes and technologies. Adequate system-level policies are also needed within an SbyD framework. These should drive the requirements for security.

The figure below, used by permission from IdenTrust, illustrates the multi-disciplinary nature of the needed governance framework where policy, technical, legal and operational issues need to interplay to form a cohesive basis strategy.



In the longer term:

4.5 Adopt an end to end systems approach

A common systems level approach to the implementation of SbyD is fundamental for secure system development. Fragmented, sub-system approaches are less appropriate because of the diversity of systems. Sub-system components need to be individually secured and resilient and adhere to a firm set of requirements set out in the design process. However, the security of the whole system is not the same as the security of the constituent parts. All attack possibilities and threat models need, therefore, to be considered at the earliest opportunity of the design phase of a system. This process needs to be at the system's core and continued through to a 'system view' which considers both the process and technology aspects of security.

4.6 Ensure transparent audit trails

Whether public or private sector, a clear/transparent audit trail of "who did what and when", in any transaction, is fundamental in an online world. Accountability, with clear entitlements and obligations (which will vary from one application to another), are integral to a trusted solution. This transparency cannot just be by way of a "Code of recommended practice". It must have contractual teeth, so that if things do go wrong, liability/financial redress can be apportioned to whoever is held responsible.

4.7 Require the certification of providers of Critical National Infrastructure Services

SbyD implies "minimum operating requirements" (MOR's) to which providers must adhere. What they do over and above the MOR's will depend upon application and competitive positioning. Rather than repeating costly and time consuming exercises that have been done elsewhere, it would seem sensible for Government to adopt established criteria already used in industry sectors where a high degree of reliance and security is integral to daily operations (e.g. banking / defence sectors).

4.8 Work with business and academia to put principles into action

As principles migrate into action, they cease to be notional/academic, but become real and tangible and carry liabilities, obligations, privileges and entitlements. The SbyD approach should not be left to the public sector, let alone regulators, to drive. It needs to be driven in partnership with commercial entities, well practised in managing and carrying the operational risks which go with critical infrastructures such as the national and global payments infrastructures. For example the payments industry is not about moving money itself, but about moving electronic data which represent value. Governments do not run payments systems. They outsource them to those who run some of the world's most sophisticated and secure real-time systems.

5 Policies must be based on Sound Professional Principles and Practice

Recommendations: the basis of a workable policy

a. Cabinet Office/NAO/Audit Commission/OGC and other planning/procurement guidelines (political and professional) to call for clear statements of the level and nature of security, reliability, resilience and integrity required in any new programme or project and the techniques to be used to check that it is indeed delivered. Ensure that this is also reflected in the procurement and performance monitoring requirements and is not left out of contracts – nearly always a false economy.

b. Create third party services to enable such audits and monitoring to be carried out, including the provision of databases of already audited products and services to enable such services to be more widely used at affordable cost.

c. Trade associations to look at the means of organising co-operation in the 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 – also working together across sectors.

d. There is a need for a common recognition, at all levels from policy to day-to-day operations, that people processes are more important than technology.

e. 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.

f. Government and policy makers should focus on creating the conditions conducive to market-based change using proven methods of auditing, certification and compliance to standards, to achieve security by design:
   - Capture the overall security requirements of the system, both constituently and holistically. The focus has to be on the end-to-end system.
   - Undertake and mandate adequate risk assessments on the system of systems, systems and sub-systems including the interconnections.
   - Assess the security of a system as a whole including cascading effects emerging from interdependencies and interoperability with other systems.
   - Promote security as common system-level problem such that everyone is required to contribute to its holistic solution.
     Promote the idea that security is not a government monopoly but a common good, with genuinely shared responsibility.

g. Government, professional bodies and education and training providers should co-operate to bring standards, accreditations, qualifications and education into line with what is needed and to ensure management understanding.
   - Promote flexibility and adaptability to respond to newly emerging threats, with tiered communication across government and industry on threat trends which better reflect levels of trust and security clearance (individual as well as corporate).
   - Promote the active management (as opposed to denial) of conflicting requirements (security vs. cost, security vs. functionality, security vs. usability).
   - Support the education efforts of key stakeholders including industry, academia and professional bodies.

- Encourage professional bodies such as BCS and IET to review the standards of competence and integrity they expect of their members and work with the UK chapters of the international security bodies to improve the quality, and control the cost, of registers of current parishioners.
- Encourage accounting bodies to produce professional guidelines on the means of valuing the difference between secure and insecure systems.
- Raise awareness of cyber-security, including current threats and mitigation capabilities, conveying what is realistic and linking solution development with legal, social and economic issues.

h. Identify appropriate security development standards such as ITU/T X.805 and identify methods for adding to standards, replacing them and keeping them up-to-date to ensure SbyD is embedded for all applications and systems, including beta versions.

The HMG Security Policy Framework[xxiii] 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 customer driven operations such as the Jericho Forum.

---

[i] http://www.cabinetoffice.gov.uk/media/cabinetoffice/csia/assets/dhr/ia_coleman080626.pdf
[ii] http://www.hm-treasury.gov.uk/poynter_review_index.htm
[iii] http://www.mod.uk/DefenceInternet/AboutDefence/CorporatePublications/PolicyStrategyandPlanning/ReportIntoTheLossOfModPersonalData.htm
[iv] http://www.cabinetoffice.gov.uk/media/cabinetoffice/csia/assets/nia_strategy.pdf
[v] http://www.cabinetoffice.gov.uk/reports/data_handling.aspx
[vi] http://www.cesg.gov.uk/products_services/iacs/iamm/media/iamm-assessment-framework.pdf
[vii] http://www.cardwatch.org.uk/images/uploads/publications/Fraud%20the%20Facts%202009.pdf
[viii] http://www.garlik.com/cybercrime_report.php
[ix] http://www.BCRC-uk.org/filelib/inhibiting_enterprise_FSB%20fraud_online_crime.pdf
[x] Ibid
[xi] http://www.getsafeonline.org/media/GSO_Cyber_Report_2006.pdf
[xii] http://www.icann.org/en/compliance/reports/whois-accuracy-study-17jan10-en.pdf
[xiii] www.cctmark.gov.uk
[xiv] www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/165i.pdf
[xv] http://www.eurim.org.uk/activities/pubproc/0909-Good_Practice_in_Procurement.pdf
[xvi] http://www.eurim.org.uk/activities/ig/voi/voi.php
[xvii] http://www.opengroup.org/jericho/
[xviii] Dr. Eugene H. Spafford, Purdue University, testifying before the United States Senate Committee on Commerce, Science and Transportation, March 2009.
[xix] http://www.eurim.org.uk/activities/ig/idg/idg.php
[xx] Boyd, Clark (30 July 2008). "Profile: Gary McKinnon". BBC News. http://news.bbc.co.uk/2/hi/technology/4715612.stm.
[xxi] http://www.law.ed.ac.uk/ahrc/SCRIPT-ed/vol6-1/mowbray.asp
[xxii] http://kantarainitiative.org/
[xxiii] http://www.cabinetoffice.gov.uk/spf.aspx