



“Security by Design”

...we need a fundamental change in market behaviour

EURIM/UK
October 2010

Hosted by: Information Society Alliance (EURIM)

Event Sponsors: CSC, De La Rue, Cisco, Cassidian

Security by Design

<http://www.eurim.org.uk/activities/ig/sbd/sbd.php>

Chairs: Carlos Solari (CSC), John Bullard (IdenTrust), Richard Goodall (Cassidian), Paul Wilson (DeLaRue)



Alcatel-Lucent

BCS

Cassidian

Fujitsu

IBM

IET

IISP

IISP

ISACA

ISC2

ISSA

Jericho Forum

Logica

UK Payments

And all other governmental participants who contributed to and monitored this paper

A Simple but Important Message



- The SbD team – it's our collective message...
...representatives from industry and government
- From the report...the evidence is clear – security more costly – ineffective in its assigned task when an afterthought
- Security by design (SbD): we know what to do...security be designed up front – but how to change engrained patterns?
- It's already begun – but we need to speed it up ...a role for government and industry



A Message with Great Urgency – and A Plan to Change

- Security by Design -

- ➤ **Society increasingly reliant on complex ICT systems – security an after thought**
 - Transforming to greater dependency: Convergence, Online Business Models, Cloud
- ➤ **Costly – ineffective – and puts society at great risk – we have all seen the news**
 - Plenty of studies to confirm what we already know, each month we learn yet more
 - *In response (£650m) from Strategic Defence & Security Review Oct 2010: “Develop a transformative programme for cyber security, which addresses threats from states, criminals and terrorists, and seizes the opportunities which cyber space provides for our future prosperity and for advancing our security interests”*
- ➤ **Security has to be built in – from start – affordable and effective as needed**
- ➤ **No Easy Task: A role for government – regulators – professional bodies**
 - Change how we buy technologies – security designed in
 - Change how we integrate them – put them into operation – certified fit-for-purpose
 - Stating up front: ***“must be proven (independently) secure to specified standard”***

● It begins – one of the largest pharmaceutical retailers in US

- **Contracted for Internet-facing web application – with PII**
- **On receipt... contracted a forensics evaluation**
- **Discovered...full of well known vulnerabilities**
- **Refused to pay for “vulnerable software”**
- **Escalations – Lawyers and Bosses**
- **Loser: developer - cost to redevelop, confidence lost**
- **Winner: retailer – no cost to patch/remediate/disclose PII losses, confidence gained...behaviour changed!**





It begins: One of India's major telecoms...RFP to industry



“[ISP serving] 75 million users...[the RFP is] **necessitated by changes in telecommunication license conditions for telecom Licensees mandated by the Licensor (Department of Telecommunication)**”

“...[the company's] intention is to engage two or three **network security accreditation** agencies for a two to three years time frame on unit rate contract basis.”

“This requirement is indicated by the large numbers and diversity of **network equipments deployed & to be deployed in India.**”

An industry undergoing change...

...to SbD...by the regulators



It begins: UK government department has to re-design its IT architecture



- **Modernisation of corporate IT (infrastructure, networks and desktops)**
- **Restricted secure environment of 6000 users**
- **Recognised significant areas of vulnerability in the design after 18 months**
- **Consequence: unable to connect to the government secure intranet until issues had been addressed – major issue**
- **Major delays in implementation of 12 months with significant cost implications (£m's)**

Security by Design

<http://www.eurim.org.uk/activities/ig/sbd/sbd.php>

Chairs: Carlos Solari (CSC), John Bullard (IdenTrust), Richard Goodall (Cassidian), Paul Wilson (DeLaRue)



Alcatel-Lucent

BCS

Cassidian

Fujitsu

IBM

IET

IISP

IISP

ISACA

ISC2

ISSA

Jericho Forum

Logica

UK Payments

And all other governmental participants who contributed to and monitored this paper