Personal Internet Security

House of Lords Select Committee Inquiry
Report: August 2007

Dr Richard Clayton

UKNOF9, London
14th January 2007
My rôle

• I was “specialist adviser” to the Select Committee, which meant I assisted them in understanding what the issues were, who they needed to speak to, and I helped ensure that the report was technically accurate.

• However, report and recommendations are the Committee’s responsibility and I am not even obliged to defend it!
Witnesses

- Government & EU: civil servants and ministers
- Industry: ISPA, ITSPA, APACS, JANET
- Police: Met, ACPO, SOCA, CEOP
- Very busy one week trip to the USA
  - FTC, Team Cymru, eBay, Microsoft, Cisco & more
- Academics and Experts
  - Bruce Schneier, Linda Criddle, Ross Anderson, Alan Cox, Mark Handley, Nick Bohm, etc etc
Government Response

- Mostly No

- Government believes that more bad things are happening more because more people are using the Internet

- Government doesn’t believe case for breach notification law has been made

- Government thinks things are basically OK!
Who is responsible for security?

• Pinning it on end-users is “unrealistic and inefficient” {Govt & ISP approach is rejected}
• Should be a kite-mark for “[more] secure” ISPs
• ISPs should be held responsible for outgoing traffic (once notified, “mere conduit” lapses)
• ISPs get a short term immunity if their own monitoring spotted the bad traffic
Understanding the problem

• No numbers, no definitions, no clarity
• Government should arrange for coordinated data collection of eCrime events with a widely agreed classification scheme
• Research Councils should work with industry to create multi-disciplinary centres to research security issues
  – along lines of CITRIS, located at Berkeley &c
Incentives for “business”

• Businesses not doing enough about security
• Banks should be liable for electronic losses (qv Bills of Exchange Act 1892)
• Government to accept principle of data breach notification and scope a (UK) statute
  – Needs workable notions of breach and accessibility
  – Mandatory central reporting of notifications
  – Clear rules on form and content of notifications
Incentives for “software vendors”

• Want modern approach to default security settings, security messages, automated patching
• Want to see moves (at European level) towards a vendor liability regime for software where negligence can be demonstrated. In longer term comprehensive liability/consumer protection regime is needed
User education

- Avoid multiplicity of websites, perhaps making getsafeonline.org into a portal
- OFCOM to make step-change on media literacy
- OFCOM to develop kite-marks for security software and social networking sites
- DCSF to identify and promote education of adults about online security & safety
Laws

- Review ICO resources and “two strike” approach. Increase penalties within DPA.
- Make hiring a botnet an explicit offence
- CPS to publish guidelines on CMA prosecutions to avoid stifling research
- Ratify the Cybercrime Convention
Policing

- Develop unified web-based reporting of eCrime
- Review scheme for reporting banking losses to the banks and not to the police.
- Create national network of computer forensic labs (with significant central funding)
- Government to fund the central eCrime unit
Oddments

• No prospect of re-designing Internet, but research into basics should continue.

• VoIP should be allowed to provide a “best efforts” 999 service and should not be regulated as if it were POTS

• Train magistrates and judges on eCrime and, in particular, on likely meaning of unsupported credit card usage evidence
Caution

- Committee are experts and highly successful in their own fields. Received a great deal of evidence both written and oral and met with almost everyone necessary to understand issues.
- Unwise to dismiss the report just because you don’t like a conclusion – it’s what intelligent people conclude from looking at what is currently happening and what is currently done.
Headlines

• ISPs to be liable for ongoing bad traffic
• Business to notify of data security breaches
• Vendors liable for software flaws (eventually)
• Banks to be liable for online theft from accounts
• Website reporting of eCrime (cf IC3)
• OFCOM to address media literacy
• Kite-marks to distinguish the safe and secure
Personal Internet Security

http://www.publications.parliament.uk/pa/ld200607/ldselect/lscotech/lscotech.htm