Is This Really Progress?

Michael Barwise

A UK Cyber Security Strategy has just been released by the Cabinet Office. The first thing I noted was that seven of its 43 pages are have a solid colour background but are otherwise blank - that's 16 per cent completely wasted space. But as I read on I gradually came to the conclusion that this figure was something of an under-estimate of the wasted space in it.

It's a very plausible-looking document at first sight. It's full of little graphs and sound-bite quotes from apparently authoritative sources, but there's not much meat on the bone. After three pages discussing the significance of "cyberspace" to society, a four page section on "changing threats" completely fails to discuss the specifics of any actual threats or changes in threats, even in a non-technical way. However it does succeed in thoroughly confusing the private, corporate and governmental threat spaces, and it preferentially emphasises the last, despite acknowledging in passing that the corporate threat space is the greatest current problem we face. The bulk of the strategy essentially focuses - insofar as it focuses at all - on government security, around half the proposed budget being allocated to *"... enhancing the UK's core capability, based mainly at GCHQ at Cheltenham, to detect and counter cyber attacks."*

Although a single paragraph on page 25 states *"80% or more of currently successful attacks exploit weakness that can be avoided by following simple best practice..."* the best this strategy has to offer the wider public in response to this reality seems to be implementation objective 1:18. *"Support GetSafeOnline.org to become the single authoritative point of advice on responding to cyber threats."* Now I have supported the aims of GetSafeOnline from its very inception and it does a good job at a very basic level, but in its current guise I feel it has a long way to go before it can effectively fulfil that brief for the whole population at risk. Currently, it raises concerns but is not detailed enough to resolve them for the non-expert, providing almost no technical guidance. A great deal of time and resources will be needed to change this significantly.

The mindset behind this Cyber Security Strategy is clearly dominated by anti-terrorism and anti-espionage, fields where directed attacks are common and a certain level of sophistication is sometimes, but by no means always, exhibited by both attackers and defenders. But the biggest security problem we face day-to-day both nationally and internationally is not high-tech online espionage or "cyber warfare". It's fragile e-commerce, due not to the expertise of attackers or sophisticated attack vectors but to ludicrously sloppy defences. Indeed the government's own head of MoD cyber security Major General Jonathan Shaw recently commented *"The biggest threat to this country by cyber is not military, it is economic"*, adding *"about 80 per cent of our cyber problems are caused by what I call poor cyber hygiene ... Many of them would go away if our cyber hygiene was better."* He didn't mention that the majority of this 80% would go away if we were able to create software that wasn't littered with stupid programming errors, but this is ultimately where most effort and resources should really be expended.

So at a time when, among the rising deluge of breaches, NASDAQ was recently described as "easy pickings" and RSA and DigiNotar - two custodians of fundamental trust relationships on the web - were infiltrated well-nigh effortlessly with international-scale repercussions, one has to ask whether *"£650 million of public funding for a four-year National Cyber Security Programme"* is best spent on more law enforcement and new ways of combating relatively rare if sophisticated targeted attacks, or whether it should preferentially be used to address the real source of our greatest insecurity - widespread failure by both commerce and government to address the most basic established principles of information security. Whether indeed a substantial budget ought to be allocated long-term - as I believe it should - to the education of competent programmers. I find the complete absence of this fundamental requirement from the strategy deeply disappointing. This strategy has largely missed the boat - unless of course it's merely an attempt to justify further investment at GCHQ in a time of cutbacks by scaring us into acquiescence with the spectre of the überhacker regardless of the real issues.

Originally appeared on the Infosecurity Network, November 2011