The $64,000 Question

Michael Barwise

This morning the radio news reported that social workers now spend so much time filling in forms and "ticking boxes" that they don't have much time to check on the circumstances of vulnerable children. This was ascribed to a process of accretion - "good ideas" being incorporated over time into a growing body of controls, apparently without coherent oversight. But it's interesting that the controls seem to have primarily emphasised extensions to documentation rather than to activity.

That brought to mind a fascinating presentation I attended recently on the EMV standard that specifies the protocols used in chip and PIN transactions. It's some 4,000 pages long, but provides little or no guidance on security or even on the specifics of implementations. A typical result, in the case of one UK implementation, is a bit field that can indicate "PIN verified" and "terminal not present" simultaneously. And the presenter - a researcher from the Cambridge University Computer Laboratory - described to us a viable "man in the middle" attack that relies on rather obvious deficiencies in the card-to-terminal dialogue, commenting that the standard has grown like Topsy until it's become extremely complex, but it remains ambiguous.

A picture started to emerge on examining an invitation to a seminar on the risks of fast-track certification under ISO 27001 - a practice I've always been worried by. Reading past the headline I encountered the phrase "*Gaining certification in Information Security is a daunting task*" - which worried me even more, as in reality, outside government and military circles, there is no certification in information security. The certification obtained under ISO 27001 is not in "information security" but in "information security management" - and information security management on a very specific but superficial model that mandates the maintenance of some twenty documentation sets describing the outcomes of decision processes but nowhere specifies - or even provides guidance on - robust methods for ensuring the adequacy of those processes or the quality of the resulting decisions.

The picture was completed on reading "*Information Assurance and SMEs: Research Findings to inform the development of the IASME model*" - the results of research conducted by the University of Worcester with the UK National Computing Centre. This report largely confirms the current assumptions about SME security awareness, albeit somewhat over-emphasising the "outsider threat" - not surprising considering one of the authors is ex-CESG. But overall, quite a good piece of research. What brought me up short and staggering, however, was the statement in the conclusions that "*Those organisations that are now in a position to do so should therefore be at least aspiring towards ISO27001 compliance or even full certification to give them the satisfaction that they are protecting their precious information assets to the highest available standard.*"

Quite apart from the solid fact that less than 500 out of over 1.1 million UK corporates are currently certified under the standard, nothing in ISO 27001 ensures that your information assets are actually protected. The standard just prescribes what processes must be in place to manage their protection - not how the processes should be designed or implemented or how to verify that they actually work. Despite which it seems "compliance" can now exculpate in case of breach, independent of actual security.

Which brings me to the $64,000 question. Which really matters more, compliance with a prescribed process or the quality of the result? If we agree the latter is the more important, we need very much more detailed (and expert) guidance on how to improve the quality of our decision-making, for that is where the real problem lies. Research by Ponemon/Accenture published in June 2010 found that almost 80 per cent of all data breaches are due to internal process or systems failures, rather than to wilful acts. But malice - from outsider threats to sexy vulnerabilities and attacks - still dominates infosec thinking. And I should add that most information security policies I've seen are essentially ineffective - except as "present and correct" documentation come audit time - for the simple reason that they don't address enforcement adequately.

So our top infosec priority is make sure our policies and procedures actually work - that they address real problems and provide effective solutions to them. That means we'll have to admit we're currently very bad at making risk and policy decisions and we'll have to get much better at it. But first we must give up covering our asses with reams of waste paper and kidding ourselves that protects our information assets.

Originally appeared on the Infosecurity Network, February 2011