Why we Find Infosec Hard

Michael Barwise

A coincidence occurred recently that may throw some light on the thorny question of why we find infosec so hard. We clearly do - the threat space is growing, the number and significance of breaches is rising, and the bad guys seem to be winning hands-down, despite a great deal of cunning technical countermeasures.

My attention was drawn to a very interesting report by Chatham House entitled Cyber Security and the Critical National Infrastructure. One of its main findings was that "*that there appears to be no coherent picture or sense of what constitutes a vulnerability, or of the likely severity of the consequences...*" and indeed "*no agreement on the nature and gravity of the problem that is either so compelling or so widely accepted as to catalyse a society-wide response....*" I have suspected this from bitter experience as a consultant, but it's striking to find one's cynical viewpoint justified at the very top of the security pyramid. The report identifies the problem and enumerates many of its symptoms. It also offers general guidance on what might be needed to alleviate those symptoms. But the one thing it doesn't really delve into is why the problem exists in the first place. To me that's the most important question. Reading the report carefully, I felt that the few comments it quoted from interviewees, such as "*organizations are bad at defining what they want people to do*" and "*there is too much bad stuff in cyber space, and it's blended too much with the good*" did little to get to the root of the matter. Then it dawned on me what at least one of the major contributory factors is.

My attention was drawn to this report by a posting on Linkedin. This led to a blog summarising the report but not linking to it. A link in this blog actually led to another secondary source that summarised the report quite similarly and again didn't link to it but to yet another secondary source. However my independent Google search raised the original without any effort at all. I've noticed this phenomenon in passing almost daily - the vast proliferation of parasitic web sites - "parasites" if you will - that replicate information iteratively - either verbatim or in brief summaries without referencing their primary sources. They range from the numerous identical open source help sites to "news" sites like the four that didn't link to this report.

Nevertheless until now I hadn't really connected the practice with our infosec problem - it took the coincidence of this chain of blogs and the content of this report to trigger my understanding. The fundamental issue seems to be a shortage of enquiring minds among the defence. I have to ask how many people who saw the Linkedin posting actually took the trouble to locate and read the original report rather than being content with three rather similar grossly simplified rehashes of its executive summary. Almost none I guess. And as I've said, this is a commonplace scenario.

The adversary, on the other hand, has access to some of the most enquiring minds in the sphere of technology - people who have learnt the machine level internals of operating systems and applications better than the developers, people who understand human psychology at a practical level better than most qualified psychologists. And people in both categories who are prepared to exercise extraordinary patience, pay huge attention to detail and work very hard indeed. Our problem is - we don't want to do any of these things. We, the defenders, live by preference in a superficial world of tweets and second-hand snippets, expending the minimum of effort on everything we do. Indeed even this otherwise excellent report - having identified the vague and uncertain way we manage infosec as the root of the problem - concentrates exclusively on "things that could be done", ignoring the question of how well or badly we might do them. The bitter truth is that while we continue to think in our familiar superficial and slapdash manner, whatever defences we try to muster we aren't going to be as effective as the bad guys - indeed most of the time we're merely performing perfunctory first aid on a dying patient. Time for a change of approach maybe?

Originally appeared on the Infosec Reviews blog, September 2011