Risk Decision Calibration

Michael Barwise

One of the biggest problems in information risk management is lack of calibration of the decision process. This results in "random output" - inconsistent and inaccurate risk decisions. It stems from several causes including unstable and/or ill-defined probability distributions of adverse events and lack of evidential support stemming from the rareness of events and the secretiveness of victims.

But the overriding contributor to inconsistent and inaccurate risk decisions is failure to allow for intrinsic heuristic biases that interfere with objective thinking about risk. This is at least as important a psychological problem as the mindset of "users", as if you make poor risk decisions, the policies you derive from those decisions are unlikely to protect you even if people do follow them. Two very useful books that cover risk judgement from this perspective are Kahneman, Slovic & Tversky, Judgement Under Uncertainty, Cambridge UP 1982, and Morgan & Henrion, Uncertainty, Cambridge UP 1990.

I have frequently commented that one of our biggest problems is the relative infrequency of infosec incidents. This leaves us trusting in the quality of our risk decisions, as it's usually possible to explain away an occasional incident that occurs despite our controls as an "exception". If incidents were much more frequent we would eventually be forced to accept that our risk decisions (the foundations of the whole edifice of defence) are mostly hopelessly wide of the mark. Then we might have the incentive to do something about it.

Absent such a flood of breaches, another aspect of human psychology - unbounded (even if unfounded) self-confidence - prevents us recognising the poor quality of our performance. Our greatest threat is that the adversary doesn't suffer from this delusion. Why not? The adversary is motivated by potential gain. But we're only motivated by preventing loss - so we're perpetually on the defensive. It's yet another psychological issue, and to paraphrase Yoda "that is why we fail". Sun Tzu probably said something about this too, but he's over-quoted so I'll resist the temptation.

Infosec is not a technical domain - it's a human domain with some technical aspects. It's therefore imperative for the infosec practitioner to have a solid understanding of how the human mind works - not just the mind of the "user" but first and foremost their own mind. Without that, the practitioner cannot calibrate their thinking and become objective.

As to whether this is asking too much, it's a prerequisite for success and the penalty for its absence is failure. Failure is a free choice, but increasingly attracts penalties.

Originally appeared on the Infosecurity Network, February 2012