Quis Custodiet

Michael Barwise

Quis custodiet ipsos custodes? - Who guards the guards themselves?
(Juvenal c. AD 100)

This applies just as much to business decision-making as it does to the persons and politics it was originally aimed at. The concepts Uncertainty and Trust, Uncertainty and Credibility and Accountability, Enforcement, and Risk are themselves necessary components of the risk judgement. "How right am I likely to be?" must always be part of the decision process. That's why we so desperately need the missing decision process standards in order to make our risk decisions at least consistent. Then we might be able to move on to making them effective.

But global formal standards have two critical failings. First, they have enormous inertia built in, so if some aspect of such a standard is found to be deficient it can take literally years to correct it. Second, the guidance provided by a global standard can only be as good as the understanding and motivations of the people who contribute to the standard. I've seen a steady decline in both the informativeness and the quality of both ISO and British Standards over the last 20 years or so, with a strong indication that adoption rate and certification paths now dominate over efficacy of guidance - witness ISO 27001, which is not by any means the gold standard for information security it's advertised as. It's primarily a very clunky and top-heavy audit preparation process for a minimum baseline level of infosec, and it's perfectly possible to fulfil the audit requirements while remaining critically insecure. Having participated in discussions on the conversion to ISO, I got the impression that BS 17799 became ISO 27001 primarily as a promotional ploy, as there's a huge market for certification consultancy and audit, and international acceptance would increase that enormously. Alignment with ISO 9000 was one of the requirements for acceptance, so ISO 27001 landed up with the crashingly obvious and rather useless "Plan Do Check Act" principle instead of some solid guidance on how to get infosec risk judgements right.

So this is where quis custodiet comes in. Until everyone from standards developers to front-line IT folks is singing from the same hymn sheet, we aren't going to be able to trust the risk management that emerges. I'm not saying that any of these echelons are trying to block or thwart anyone's activities, but while they're all primarily seeking their own ends they're not really pulling together. Trust cannot be demanded or regulated for - it's born gradually from experience of successful outcomes. That means risk decision methods need to be defined taking into account the realities of where we go wrong and individual risk decisions need to be fully documented with evidentiary support, validated against results. Only then can proper review and improvement take place.

Just in passing, it's worth noting that IT and infosec risk are managed much worse than, for example, nuclear, aerospace or chemical engineering risk. We're therefore not talking about something that's can't be done, but about something that needs better-equipped people doing it.

Originally appeared on LinkedIn, November 2010