

23 May 2008  
MH

*A man was searching for something on the pavement under the gaslight. A pedestrian passed by, stopped and asked him: "Have You lost something?". "Yes, my keys", our searcher said. "Did You lose it just here under the gaslight?", the pedestrian asked. Our searcher answered: "Not really, I lost it in the dark end of the street. But it is much easier to search here under the gaslight."*

## **Comment on "Security Economics and the Inner Market"**

Having read the ENISA proposal please let me address my wholehearted support to the ENISA recommendations. I am impressed of the report quality and agree heavily to the approach that introduction of statistical measuring and reporting will serve as an eye opener and lead corporate firms and public administrations towards a more rational behaviour according to information security.

When we are dealing with privacy and losses of intellectual property, it is widely accepted that the incentives to report damages for many reasons are very low. Neither CISO s nor CFOs are tempted to report experiences with industrial espionage. Thus the losses will not figure in annual reports and the rationale of counterfeit them tends to evaporate.

As a consequence the latent damages of breaching confidence tend not to be reported and consequently only very rarely estimated. Even if the ENISA recommendations were implemented as a whole the risk of still having lost keys in the dark end of the street might seems to be relevant.

The legal action of reporting privacy breaches will into some degree turn out to be helpful - according to the experiences from USA. However, the breach of confidence deals with many other pieces of information than just references to persons, and the value of the losses may probably differ from the value of the losses due to privacy breaches.

International IT Security Standards tend to underestimate or even ignore the latent and inexperienced breaches of confidence.

One might argue that the uncertainties of such estimation could be worse than nothing. Nothing is almost what we already have. The CISOs have so far had very low success in introducing measures against losing confidence for several reasons. One of the most

obvious is the fact that the cost will be manifestly booked while the loss and its further consequences still will be latent.

This leads to the question: Is it possible to produce valid estimates on confidence breaches when the amount of observations is low and the size of losses is not standardized?

According to the first, an actuary's approach might be appropriate.<sup>1</sup> According to the latter, it might seem reasonable to formulate a procedure to estimate the both the short term and the long term losses due to one damage.

*This leads me to recommend ENISA to focus distinctively on the need for developing methods to estimate the spread, the amount and the size of breaches of intellectual property and thus to set another gaslight in the dark end of the street and hence to produce a recommendation for proper behaviour in this particular field in the future.*

Yours faithfully

Mikael Hertig

Direct: +45 44 78 42 54

E-mail: [hans.mikael.hertig@logica.com](mailto:hans.mikael.hertig@logica.com)

---

<sup>1</sup> See for instance Hertig Joakim, A STATISTICAL APPROACH TO IBNR-RESERVES IN MARINE REINSURANCE