

Time to name and shame?

As we all know, or at least should know, the Information Commissioner's Office can now impose fines of up to £500,000 on organisations that recklessly put their data at risk

The words 'of up to' are of significance and exactly what a 'reckless' loss of data entails is yet to be defined in practice and while the ICO should be commended for taking such an important step to instill a sense of responsibility, you do get the feeling that something is missing, says David Kelleher, Research Analyst at GFI Software.

Firm but fair

"The threat of a hefty fine and not a slap on the wrist is just what the industry needs," says David. "There have been too many instances over the past year or so where data has been lost because an organisation lacked the necessary security infrastructure or best practices or its employees were negligent enough to lose the data. Laptops left in airports, memory sticks found in bars or backup CDs lost in transit are some of the stories that have made headlines.

"Although the press has highlighted these data loss incidents and been critical of the culprits, the issue is soon forgotten by thousands of other organisations who may have felt sympathy for the guys involved but little concern, if any. After all, they would argue that they are immune to these problems and it would not happen to them.

"The ICO, in establishing such hefty fines, has acknowledged, late some would say, that many organisations are not giving enough importance to security or the data that they handle.

Just as there are organisations that invest heavily in security and give the matter the attention it deserves, there are many organisations that consider security to be a waste of time and money. In smaller organisations, unfortunately, security is often ignored or too far down their priority list because they are overly confident that they are of no interest to anyone out there or they have implicit trust in their employees. In either case, they are asking for trouble.

"The ICO, by imposing fines, is sending a stern warning to organisations to get their act together but is the 'fear' of a fine enough to push organisations into investing more in security and security awareness?"

Damp Squib?

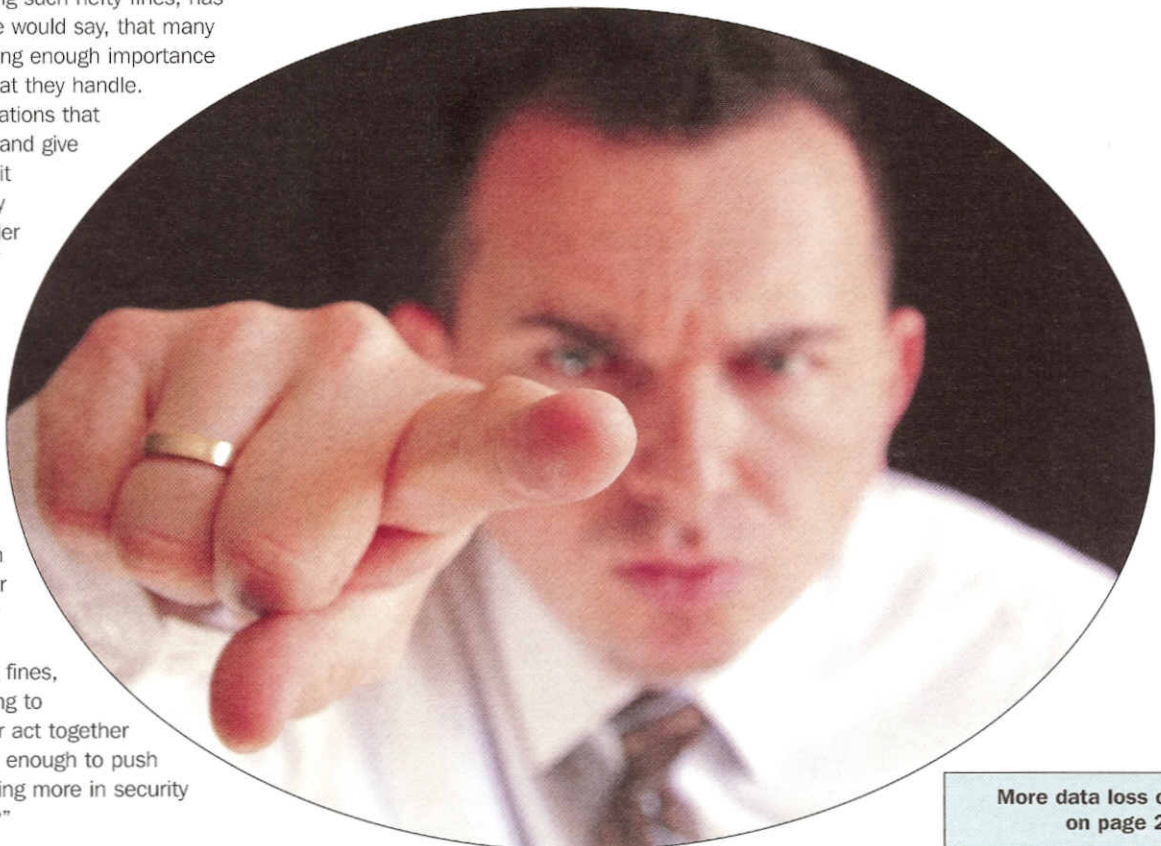
According to David: "While the threat of a £500,000 fine may be a deterrent, it may not be enough. Assuming that the maximum fine would be imposed on an organisation suffering a TK Maxx-type breach and the ensuing negative publicity would be highly damaging, smaller organisations may get away with a fine and reprimand, but little harm to their credibility and reputation. What the ICO could consider is to back up these fines with a public register which names and shames those organisations that were found to have 'recklessly' lost data.

"Companies that negligently put their own data, and that of their customers, clients and suppliers, at risk should be named and shamed in public. There are many companies that can afford the £500,000 risk, and many of these have some of the most publically-sensitive data at their fingertips. However, while the financial deterrent may not be sufficiently compelling to rule out all risks, the threat of being publically named probably will be, and works particularly effectively as a deterrent in the US.

"Organisations can ill-afford not to invest in security. There are too many threats around - from social engineering to fraud and malware attacks to cross-border cyber-crime - for organisations to ignore and do nothing.

"Those that do ignore the risks and are doing little to safeguard their data are not only harming themselves but their clients at the same time," concludes David Kelleher. "Naming and shaming in public is one deterrent that could be a determining factor in improving the overall quality of security in organisations.

What the ICO could consider is to back up the fines with a public register which names and shames those organisations that were found to have 'recklessly' lost data



More data loss comment on page 27