

# Data transmission and information sharing



Data loss incidents in the public sector have a negative impact on the reputation of government. Software AG's lead technologist **Tim Holyoake** argues that reliable electronic messaging is one way to restore faith

**O**ne of the most common concerns that our customers have raised with me over the last year has been the increasingly febrile atmosphere surrounding the issue of data loss, particularly in the public sector. When the Information Commissioner's Office published a press release in October 2008 announcing that there had been 277 self-reported data breaches in the year since the highly publicised loss of child tax credit data by HMRC, I decided that two follow-up questions needed to be asked. Firstly, I wanted to gain an understanding of how many of these data breaches were due to secure government or corporate networks being compromised, and secondly to understand the information commissioner's position on the use of reliable

messaging for the transmission of data over such networks.

Given my background in the design and implementation of products to support reliable messaging, both questions were of obvious interest, yet no-one appeared to be asking them. If a considerable number of data breaches had been due to secure networks being compromised, then it followed that there would be significant consequences for vendors such as Software AG and for the type of products and services we offer. One of our major markets is in providing reliable messaging products that utilise these secure networks for data transmission between government departments and agencies, and we have invested considerable effort over the last six years (and

continue to do so) in bringing to market products that facilitate and regulate electronic information sharing.

It was therefore fascinating to receive a response from the Information Commissioner's Office which informed me that of the 277 incidents in question, only one could possibly have been construed as a breach of a secure government network. The circumstances behind this breach involved "... a web-based virus, which had the potential to by-pass login and password protection. The vast majority of the information held on this system was information already within the public domain ..." They continue: "This [is] ... the only incident which may fall within the category of the information requested."

I would argue that a potential for harm that has been identified and acted upon does not fall into the definition of a breach of a secure network. Indeed, the answer I received demonstrates that the greatest threats to our information security do not lie in the systems, databases and networks the data is stored in and processed by, but rather in the behaviour of the individuals using that information. Lost removable media or mobile data storage devices accounted for 56 data losses, and a further 49 were due to the loss of paper documents. Theft accounted for 78 further instances, and information disclosed in error totalled another 58 items.

Psychologists working in the behaviourist tradition often discuss the relative merits of negative and positive reinforcement strategies in affecting human behaviour. Some of the understandable responses to data loss in the public sector have been to attempt to influence behaviour through negative reinforcement; in other words, punishment. These have included the prosecution of individuals who have lost information and the cancellation of contracts from some private sector organisations whose employees have done the same. More subtle forms of punishment have also been used. One government agency I visited recently had stopped individuals from using third party courier services, and was insisting that information could only be collected from their data centre by employees. This is a pretty draconian measure, particularly when you consider it could result in a round trip of several hundred miles in some instances, with all of the associated lost productivity and increased costs.

While punishment can have an obvious and immediate impact on behaviour, evidence suggests that it is far better to use positive reinforcement, rewards to change behaviour. Hence my second question to

the Information Commissioner's Office concerned their preferred means of data sharing. Their response is unequivocal: "This office would consider reliable messaging via secure networks, to be preferential to the use of removable media storage devices for the purposes of information sharing." This should be a wake-up call to us all. We need to treat sensitive information in the same way banks treat paper money. A clerk would not be allowed or need to take currency to count. By the same token government employees and contractors should not be allowed or need to move information around on removable media.

I believe that it is incumbent on trusted vendors like Software AG, who supply reliable messaging products and services which support the secure transmission and sharing of information, to work with public sector organisations to put in place mechanisms that facilitate secure and efficient means of data sharing that benefit individuals, by making their working lives easier and protecting them from avoidable personal liability. We are happy to report that government departments and agencies are increasingly using such mechanisms to facilitate the effective and regulated use of information to deliver better services more efficiently.

Software AG is actively working with our public sector customers on numerous data transmission and information sharing initiatives. The information entrusted to the care of our products includes the biographic, biometric, financial and educational information of individuals, as well as that of corporate organisations. We offer a proven range of products and services aimed at ensuring effective and secure information transmission and usage, while protecting the privacy and interests of individual citizens. We passionately believe that the behaviour desired by the information commissioner should be rewarded, by providing public servants with the capabilities and tools they need to deliver efficient services. Software AG is always happy to talk to you about our customers' experiences and work out how best to address your specific requirements. Why not give us a call? ●

-----  
 Tim Holyoake is Software AG's UK lead technologist. He was one of the designers of the Sun Software AG DIS – the most widely used reliable messaging product approved for use with the Government Gateway. Tel: 01344 403 800  
[www.softwareag.com](http://www.softwareag.com)

**“We offer a proven range of products and services aimed at ensuring effective and secure information transmission and usage, while protecting the privacy and interests of individual citizens”**

