

Bankcards or smartcards – which would you prefer?

March 2008

By Tom Rothwell, Managing Director, Medisec Software

Until a few weeks ago, organisational ineptitude appeared to be the chalice of UK Government departments or institutions, following a string of highly confidential, personal data losses.

But as the almost implausible story of Société Générale trader, Jerome Kerviel, came to light, it has become clear that no institution is unsusceptible to systemic failure.

Allegedly, the trader managed to conceal his activity by understanding how to play the system, or rather how to play two systems. He understood both where to hide his transactions and he understood how to avoid his deception triggering any warning by the bank's computer system.

In effect, a single individual with a fair knowledge of IT systems managed to cost France's second largest bank £3.6 billion.

Assuming, of course, that Société Générale had invested large sums on security processes, the prognosis is that no computer system can be deemed entirely free of security risk. And that assumption must extend to a nationally held database.

If National Care Records proceed as planned and the personal data of 60 million people are held in one place, accessible in one form or another by many thousands of people, then the potential for a 'rogue trader' is staggering.

Connecting for Health may argue against this. Access to records will apparently be granted only to relevant individuals to access relevant information. But human nature dictates that such security boundaries will be crossed.

When individuals are busy at work or need help, access to information is all too easily given to someone who is not authorised, to alleviate the problem. While the vast majority of this non-authorised activity will be completely innocent, it will happen and it demonstrates a major flaw in a system that is built on multiple levels of access to a central data store.

CfH may also argue that individuals will only be able to access those records pertinent to their own practice or at most their PCT. But as amply demonstrated, it is not beyond the wit of man to deliberately deceive complex and secure computer systems for inappropriate means. Which begs the question: is it likely that the IT prowess of CfH is that much greater than that of a financial institution the size of Société Générale?

With CfH apparently admitting to the loss or theft of almost one percent of the 430,000 NHS smartcards issued, the frailties of the system are clear. CfH state that when a smartcard is reported lost or stolen it will be disabled. But with so many cards in circulation, it is an almost impossible task to know whether all smartcards are in 'safe' hands or otherwise.

Combine the 'human factor' of IT security and the frequency of data loss in the UK and it becomes hard to believe that any system can be completely secure.

If it really is the case that no data store can be judged to be 100% secure, then the associated risks can only be minimised by reducing the amounts that can be lost. To draw a natural conclusion, data must therefore continue to be stored at a local level, removing outright the risk of data loss on a national scale.

Would it not be far more effective for GPs and consultants to exchange patient information with one another on a 'need to know' basis?

Practitioners can agree in advance which details they need, mandate one another to provide a checklist of critical clinical details and communicate them quickly, efficiently and securely using electronic means. In this way, the system will 'push' all the most relevant information towards the next consultant in the chain, rather than relying on him to 'pull' it from a central 'at risk' resource.

For the patient, first rate care is the most important issue and there are clearly benefits to having a central data store. But with 60 million records at stake, the benefits of National Care Records begin to look debateable until such a system can demonstrate much reduced risk.

And if you want to know about risk, just ask a banker.

Tom Rothwell, Medisec Software

671 Words

- ENDS -

31 January 2008

For further information please contact either Toby or Debbie at Cameron Wells Communications on tel: 0161 973 4158 or

toby.walker@cameronwells.co.uk or debbie.wells@cameronwells.co.uk