

# IT'S ALL ABOUT THE DATA

With the government regularly in the news over IT mishaps and lost data, how can you ensure data is treated securely once outsourced, asks Guus Leeuw jr, President and CEO of ITPassion Ltd

## DEAR READER, THANK YOU AGAIN

for taking the time to read this article.

In the last two months, we've covered identity servers, public key infrastructure, and storage area network technologies to enable great virtualisation possibilities.

But there's one thing I haven't yet mentioned: IT services and outsourcing. This is becoming a concern for some people with the government regularly in the news over IT mishaps in general and lost data in particular.

Managing an IT service organisation from a client point of view isn't always easy. Sometimes the client won't know what's needed, sometimes the IT service organisation doesn't know or is unable to deliver exactly what's required.

In this context, ensuring proper security is a big theme within communication, data gathering, and data management. In other words, it's all about the data, and what is being done with and to that data.

## CONFIDENTIAL DATA

Government organisations invariably deal with a lot of private data which, if it falls into the wrong hands, may cause considerable problems for many people. From identity theft to compromised credit cards or bank accounts, personal information has much value to organised criminal gangs.

Take the recent case of PA Consulting losing a memory stick containing confidential data on 84,000 prisoners. PA Consulting runs JTrack, a government scheme to track prolific offenders through the criminal justice system. The important question that the loss raises for me is this: how can a good IT service organisation appear to be so lax in complying with the Data Protection Act?

At face value, the embarrassing occurrence hardly seems the fault of the Home Office or of any other government agency involved with JTrack. But there may be an important factor in the government underestimating what security breaches might occur when dealing with external IT service organisations.

## TAKING DATA OFF-SITE

Taking the data off-site for processing might initially seem a good thing to do. But would you want anybody to be able to handle the device upon which that data sits? Where does the data actually go once it's left your premises? And how can you be absolutely sure that no tampering will take place?



the off-site testing version can be substituted with random text.

I'm currently working at an organisation in the Netherlands where we regularly deal with off-site storage of backup data. The tapes are kept in a locked case for which only two people have a key (the person who put the tapes there and the person who might need them later).

Nobody else has access to the keys or the safe in which the keys are normally kept. All tapes are always transported in locked cases which, obviously, are much harder to lose than a memory stick which could so easily fall out of a pocket.

## GET AN INDEPENDENT REVIEW

There's one final area that I want to mention. It's always good to have a second opinion about issues which may be too complex to understand or how best to handle critical information safely. The government's JTrack system may work well but the recent data loss revealed a serious vulnerability. Perhaps it might have been better for an independent IT service organisation like ITPassion Ltd to have reviewed the protection against possible security breaches – human or otherwise.

By undertaking such independent reviews, the government can usefully spend some money to

“It's always good to have a second opinion about issues which may be too complex to understand or how best to handle critical information safely. The government's JTrack system may work well but the recent data loss revealed a serious vulnerability. Perhaps it might have been better for an independent IT service organisation like ITPassion Ltd to have reviewed the protection against possible security breaches – human or otherwise”

The lost PA Consulting memory stick should, if nothing else, lead to one important rule being adopted. Raw data should always be managed in-house. If you take it off-site – even if this is still within the offices of the primary contractor – it should be made anonymous first. Then, if it's ever lost, little real harm may follow.

Although it might seem justified to test new versions of a system off-site with a copy of the live database, I don't think that's necessary these days either. As long as the data provides characteristics that the system is built to use – like full text address searches – then real data in

guarantee proper data security. Preventing possible data losses costs far less than clearing up the problems caused afterwards. In general, I always tell clients wanting to outsource their IT services that managing raw data is strictly out of bounds for us. ITPassion does not touch or handle clients' raw data. Never. Because that is, simply put, far too risky.

## FOR MORE INFORMATION

To find out more about our IT virtualisation products and solutions, please visit our website [www.itpassion.com/gt/october2008](http://www.itpassion.com/gt/october2008)