



# Managing the risks in the modern IT environment

Reading newspapers or watching the evening bulletin is not always about seeing good news. For example, the government is often blamed for IT mishaps or eavesdropping on the public. There's usually a common theme in such reports: security. What's the significance of security, data handling and IT services? **Guus Leeuw jr** provides a personal viewpoint.

OVER THE LAST FEW YEARS, SECURITY has played a big role in the IT industry. Many, if not all, computer systems require the user to login for identification. This defends them from unauthorised usage – often a common warning seen on login screens.

'Wait a minute,' I hear you say, 'Identification isn't the same as authorisation.' That, of course, is correct. For example, Microsoft understands this well enough by allowing a whole range of security policies to be applied to users and computer systems alike.

Using such security policies is the right way forward in an uncertain age: if a computer system knows who you are (it has identified you), it should certainly check that you're allowed (or authorised) to do what you're doing. This applies to starting or installing a program, as well as viewing any information online.

Most systems, however, don't cater for such finely detailed authorisation. Once you're connected to a website, it doesn't check if you're allowed to view certain content. Even worse, once you're connected to a database, it doesn't confirm you're allowed to view the stored information either.

### Systematic checks

Fortunately, some end-user applications support the systematic checking of authorisation and this is what security in the IT industry needs to focus on. For example, common lightweight directory access protocol (LDAP) systems provide a number of processes and functions to allow finely detailed identification and authorisation. However, different LDAP systems may not work too well together.

A heterogeneous (mixed) IT environment may, therefore, have two enterprise directory services for Windows and UNIX or database systems. While they will share some information, such as user ID and password, they won't often share any detailed security settings. That means their main role – centralised user and account management – is easily undermined.

You can take IT security very seriously indeed by preventing all unauthorised access. Such good levels of security can be achieved for central or local government systems as easily as it has been for private companies – systems can work effectively through use of central identification and authorisation management.

Even backups can be protected these days. For example, the online backups

taken from laptop and desktop systems can all be encrypted. These backups can only be accessed and decrypted by the original user authorised to do so. Lost or stolen systems may be replaced, and the backups safely restored.

By using central authentication and authorisation management products, truly secure systems can be developed that are virtually unbreakable. These are ideally suited for use in government – from the local town hall to a Whitehall department.

### Keeping your backups safely

Let's focus on backup and restore again for a moment. Most often, data (or even a complete system) is backed up for disaster recovery purposes. The backup tapes may be sent off-site for safe storage and, if required, quickly returned to restore lost data.

Most tapes sent for off-site storage contain some form of catalogue to identify the tape and its contents. In extreme cases of original data loss, the catalogue must hold enough information to retrieve all the stored data properly, especially if you have to install a complete new IT environment following a major disaster.

For example, backup solutions

conforming to the network data management protocol (NDMP) standard might utilise a pre-described method to store data on tapes in the form of well-quantified storage records. Anybody with an appropriate reader might potentially retrieve the data off the tape and then attempt to inspect it.

Stored tapes are, therefore, an unrecognised security risk, especially given the public's concern about recent incidents involving lost data. It would be best to encrypt the backups so that even a determined hacker is unable to read a tape's contents. That seems an important consideration given many government agencies deal with so much private data these days.

Equally important is the fraud often mentioned in the news: discarded computers shipped to some faraway location for recycling. Their hard disks may be trawled for private data such as credit card and other useful information. It would be very useful to have a program to wipe all the data securely off a PC's hard disk before disposal.

Governments around the world have taken action to support this kind of security and good security tools aren't hard to find although, generally, they're not free. In my opinion, governments should do much more to promote their wider availability.

### **Harness the virtual world**

There's another important element of the data storage infrastructure. Virtualisation breaks the links between IT components – like servers and storage – and uses fibre optic connections so they can be repurposed in a more logical or efficient way. Did you know that you can slash your annual IT costs by at least 40 per cent when opting for a virtualised server environment?

While virtualised environments support much more work as the underlying physical layer gets more powerful, a faster and better access to back-end storage systems is also required.

Speeds of up to 8Gbps are not unheard of within a storage network and even storage devices themselves may support 8Gbps connections. Running at these speeds, implementing Microsoft Exchange environments on virtualised hardware is very possible. That's especially so if you can achieve end-to-end, virtual server to storage guaranteed data paths – as if the virtual environment was a physical environment. And providing hosting for multiple government agencies starts to become feasible too.

Whether you use virtualisation or not, 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. 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.

### **Minimising external risks**

Government organisations invariably deal with a lot of private data that, 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 is this: how can a good IT service organisation appear to be so lax in complying with the Data Protection Act? Did the government underestimate the risks of using an external IT service organisation?

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 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 the off-site testing version can be substituted with random text. This is the sort of issue that could be spotted during an independent review – the risks of sending real data off-site now seem obvious.

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. We do not touch or handle client data – ever. Because that is, simply put, far too risky. ■

**Guus Leeuw jr is president and CEO of ITPassion Ltd ([www.itpassion.com](http://www.itpassion.com)).**

Taking 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? How can you be absolutely sure that no tampering will take place?