

The horse of Troy

Security should be embedded in your organisation's DNA.

A colleague and I were recently given a rather excellent guided tour of a company providing a digital service to their clients. I won't go into detail; however their work includes the collection and retention of significant levels of their clients' personal information such as the usual names and addresses, as well as credit card and other payment details.

The CIO giving us the tour was running through what, on the face of it, was an outstanding and extensive new security setup costing them thousands – from industry-strength firewall and gateway protection to the physical security of the main servers and machines; excellent.

It wasn't until we were on our way out, with the CIO explaining how seriously the company viewed security, that I noticed the nicely labelled container and its contents on the edge of the reception desk in the very busy – and public – reception area. Can you guess what was in it?

Coincidentally I was talking to a colleague later the same day whose client had been the victim of a bank phishing scam – you know the type: the criminals send you an email linking to a website masquerading as your bank's official site where you can 'log in' to your account, and they siphon off the details you enter in order to attack your real bank account. Easy money! Fortunately the scammers didn't get away with much that time. However one has to ask how this happens; the banks spend huge amounts of money securing their websites and other systems and after all, surely we all know about phishing now, don't we?

In many ways this is similar to that famous wooden horse of Troy (the one from Greek mythology, not the computer malware named after it); the one that appeared to be an

innocuous gift but contained Greek soldiers waiting to pounce. "How nice! Let's drag it inside," said the Trojans. And we all know how that ended...

But back to that nicely labelled container on the reception desk: those who guessed it was unencrypted backup tapes sitting in clear sight, clearly labelled in a public area waiting for an information thief to pop by and uplift them, were right – somewhat ironic that backups exist to save your bacon but could end up being responsible for frying you!

There's more similarity between these three scenarios than meets the eye. It sounds logical, but no matter how much is invested in security processes, systems and products, and no matter how strong the walls of your city (or digital equivalent), it's almost impossible to create a lock that can't be defeated in some way by those that are charged with looking after the key, especially if they can be convinced to give it away.

Interestingly, if you asked most users what was worse – leaving a backup drive lying around or giving someone login details to their bank's website – they'd almost invariably say the latter. However, the potential exposure of the first is significantly higher.

Whilst most banks have systems in place that don't allow large transfers without a separate verification of identity, a loss of sensitive commercial data can end an organisation overnight, in some cases destroying millions of dollars of value. In many countries a loss such as this has to be publicly notified, and companies and individuals have been sued, careers ended and businesses and lives ruined by what might have seemed like a minor lapse at the time.



Paul Matthews

Paul Matthews is the Chief Executive of the New Zealand Computer Society (NZCS), the professional body of the IT sector. NZCS is chiefly concerned with raising the professional and educational standards of ICT professionals and computing skills of the public, working in collaboration with others to achieve these goals. Before running the Society Matthews founded and managed several IT-related businesses.

Phone: +64 4 473 1043

Email: paul.matthews@nzcs.org.nz

Web: www.nzcs.org.nz

This stuff happens every single day. Security is not just about firewalls and encryption, and it's not something to be bolted onto the system as an afterthought or worried about by one or two staff. It must be present in the DNA of an organisation – part of the culture, part of induction and training, and a way of life for the entire team every day, from top to bottom. Only then will we have a truly secure system.

Oh and lastly, perhaps you might want to go and check how your backup drives are stored and handled – it may just end up saving your bacon one day. 