Identity theft IS a technology issue

BY STEPHEN WILSON

It is politically correct nowadays to claim that any particular management headache "is not a technology issue".

Try Googling that phrase in quotes – at the time of writing I got 551 hits! Every week business people tell me that risk management, for example, is "not a technology issue". Neither apparently are electronic banking, privacy or information security.

What we're really trying to say is that these issues are complex, multi-facetted and not confined to technology. No one could deny it.

But "Security Is Not A Technology Issue" has become a bumper sticker slogan, and businesses get into real trouble when they take the slogan too far.

It can have two sorts of negative effects. Firstly, ever-optimistic technologists take it as a false sign that they're off the hook. "Phew!" you can almost hear them say; "I'm glad security isn't *my* problem". And secondly, it fosters techno-fear, steering organisations away from fundamental fixes and on to imperfect compromise solutions.

Take identity theft for example. Today's Internet banking systems are vulnerable to several forms of attack. Top-of-mind of course is "phishing", where customers are spammed with bogus e-mails and invited to divulge their account numbers, PINs and so on.

In May, Gartner Research released a study showing that between 30 and 57 million Americans had received a phishing pitch. About 3 per cent of recipients responded with their personal details. Many more – nearly one in five – clicked through to a website from a phishing pitch, leaving themselves vulnerable to spy-ware (more on this below). Phishing is among the most successful online scams, costing US financial institutions some $1.2 billion last year, according to Gartner.

Phishing has become so serious that some US government agencies have advised that they will no longer use e-mail to communicate with citizens. What a tragedy for e-commerce, if we have to retreat to snail mail!

Online institutions can also fall foul of website "ghosting". Hackers have a number of tricks at their disposal for erecting bogus or ghost websites. The simplest is to register a new URL that closely resembles a real site, and hope that visitors don't notice the difference. If they're following a link in a phishing pitch then it's quite likely they won't.

More sophisticated ghosting "spoofs" or counterfeits the actual URL. Until recently we thought that SSL protected against URL spoofing. Unfortunately, flaws have been discovered which mean that the appearance of the famous SSL padlock is no longer proof that you are at the site you think you are.

Even more pernicious forms of attack are on the rise. Most worrying is the "keystroke logger", a form of spy-ware loaded surreptitiously on to a user's PC. Keystroke loggers monitor every keystroke and transmit them over the Internet to an attacker. Names, numbers and PINs are then sifted out of the key stream and used to hijack the unsuspecting user's account. Such spy-ware can infect PCs via screen-savers, viruses and phishing scam websites.

> **"There is no time left for technological complacency"**

The banking industry's broad strategy on identity theft has been to fight it on a number of non-technology fronts. Internet fraud has been painted as a small proportion of crime overall, and a problem that is probably more serious overseas. Banks so far have been able to cover the cost of identity theft within their existing risk provisions without impacting customers. Direct mail and newspaper advertising have been used to engender safer online behaviours.

For the most part, technologies to combat identity theft have been played down. Technology is generally perceived by executives to be expensive – and unfashionable.

Naturally, we haven't wanted to raise unnecessary alarm, and we did need to gather good statistics before taking long-term action. But there is no time left for technological complacency. In the war on identity theft, the conventional weapons of education, marketing, regulations and the law are about to reach their limits.

Let's admit it: security is very much a technology issue. It always has been. Moreover, our industry has been good at it. In ATM security for example, Australian banks have long led the world.

ATM-equivalent levels of safety on the Internet are some way off, and a lot will depend on software companies, computer makers and ISPs. Within the banks' sphere of influence, perhaps the most significant security initiative will be the replacement of magnetic stripes by smartcards.

It is almost impossible to clone a smartcard, so they are the best known countermeasure to skimming. And the cryptographic chip within – the thing that makes them "smart" – can also run the new Internet payment protocols like MasterCard *SecureCode* and *Verified By Visa*, to make Internet banking and e-commerce safer. As "two-factor" authentication, smartcards protect against keystroke logging because a thief needs the card as well as the password.

What's less widely appreciated is the fact that smartcards also offer effective new ways for institutions to protect their own identities online. Smartcards can strengthen SSL to prevent website ghosting. And they could be used to secure all electronic communications sent out by banks.

The business case to roll out smartcards has proven elusive for Australian banks. But by using smartcards to safeguard their precious online customer relationships, restoring confidence in the Internet channel, the cost-benefit equation starts to look a lot rosier.

Key points

- **It's time to move beyond the bumper sticker slogan "security is not a technology issue"**
- **In the war on identity theft, education, legal and regulatory weapons have reached their limit**
- **Smartcards protect both institutions and customers from identity theft.**

■ **Stephen Wilson is a leading international authority on identity management and information security. In early 2004 Stephen established Lockstep Consulting to provide independent advice on security, authentication, e-business risk management, and privacy. Lockstep is also developing smartcard based solutions for combating identity theft and managing anonymous transactions.**

swilson@lockstep.com.au.