



IN SELECTED QANTAS INTER

QANTAS

Visit qantas.com

theage.com.au

THE AGE

 [Print this article](#) |  [Close this window](#)

The cost of losing yourself

Conrad Walters
November 16, 2008 - 11:07AM

Privacy breaches are shaping as the new pandemic infecting business stability, reports Conrad Walters.

The lapses came at a rate of one a week: hundreds of credit card receipts from a Bondi Junction chemist are strewn across Mascot Oval; names and dates of birth for 3500 customers of a Sydney restaurant are inadvertently attached to a mass email; detailed financial records for Aussie Home Loans customers are dumped in an unsecured bin; and, most worrying, a Tax Office CD of documents about 3122 taxpayers vanishes after reaching a courier.

And those losses of personal information, all from last month, were the ones made public.

October, though, was not alone as a bad month. A recent survey by the computer security company Symantec found 79 per cent of Australian businesses know they have lost sensitive information about themselves or their customers.

The survey of nearly 200 businesses with more than 100 employees shows data loss is anything but rare. Forty per cent of companies that lost information acknowledged six to 20 losses in the previous year. Eight per cent admitted 100 or more instances. Data losses cost one industrial company \$8 million.

What is going astray? Everything from customer and financial details to employee records and competitive intellectual property. The biggest causes: lost laptop computers and mobile phones, and human error. Lower on the list, but still statistically alarming, are corporate espionage, hacking and insider sabotage.

"What the survey results show is this is not hype," Craig Scroggie, regional managing director of Symantec, says. "This is a real and present challenge."

Certainly it will assist the bottom line for Symantec, a seller of software to monitor documents and protect data, but the risks to companies and consumers are enormous.

Australia does not require companies or government departments to reveal breaches of personal information to the people affected. It is not possible, therefore, to know precisely the number of stuff-ups and the number of people affected, but there are clues from overseas.

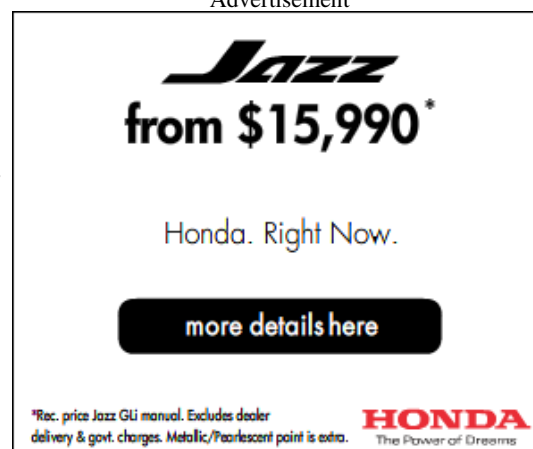
In Britain last year government officials lost two CDs containing birth dates, addresses, bank accounts and national insurance numbers for 25 million child benefit recipients.

In America, 44 states have laws requiring businesses to inform consumers when personal details have been compromised and the Privacy Rights Clearinghouse (www.privacyrights.org) monitors such breaches.

A scan of cases from recent weeks is revealing. A Seattle school district inadvertently released 5000 social security numbers (similar to a tax file number) to a union and a US State Department breach allowed the theft of details from 400 passport applications.

An Ohio health insurer lost 11 computer disks with personal data on 36,000 retirees and employees; a burglary at a Californian risk management company resulted in the theft of details on 5700 workers who had filed compensation claims.

Advertisement



Jazz
from \$15,990*

Honda. Right Now.

[more details here](#)

*Rec. price Jazz GLi manual. Excludes dealer delivery & govt. charges. Metallic/Pearlescent paint is extra.

HONDA
The Power of Dreams

Since it began monitoring breaches in 2005, the Privacy Rights Clearinghouse has tallied more than 245 million compromised records.

Bill Hay, a Queensland detective superintendent and expert on computer crime, says Australia is no safer and that "it's going to get worse". Data theft, Hay fears, will boom because of profits in individuals and companies trading sensitive information to obtain personal identities and corporate secrets. Australia's attitude, he says, is "a wait-and-see approach, as opposed to a fraud prevention approach".

Data losses have grown exponentially as technologies have made more things possible. Symantec's Scroggie sees the risk daily because he spends most of his time out of the office with a laptop containing payroll records, patent applications, tax returns and more. His files are encrypted and backed up, but that's not true for everyone.

Information walks out of government and corporate offices via every conceivable avenue: burned to DVDs, downloaded to USB drives, copied to MP3 players and stored on Blackberries. It travels by email, across the web and over wireless networks.

One result? Identity theft. According to Personal Fraud, a landmark Australian Bureau of Statistics study in June, 124,000 instances of ID theft were reported in the previous 12 months.

For business, the risks are potentially catastrophic. A seller of computer security, McAfee, surveyed 1400 large companies in the US, Britain, France, Germany and Australia, and found 60 per cent reported losses of confidential data in the preceding 12 months.

"Even more frightening," the McAfee report says, "a full third of them believe a major breach could put them out of business." The McAfee investigation predicts "it's only a matter of time before a high-profile company, perhaps a squeaky clean one bursting with integrity and good will, is brought to its knees by a breach".

A global study by Ernst & Young explains in *Moving Beyond Compliance* that the great concern of businesses is the loss of reputation. That is, they fear their customers will go elsewhere if news of a breach becomes public.

Against this backdrop, the Australian Law Reform Commission released recommendations in August for an overhaul of the Privacy Act, in light of the remarkable transformation in technology during the act's 20 years. When it began, laptop computers resembled suitcases and mobile phones house bricks. Personal risk associated with them was more likely to refer to muscle injuries rather than lost information.

The commission's report - all three volumes, 2700 pages, 74 chapters and 4.8 kilograms - contains a call for mandatory notification of lost personal information. The 295 recommendations include a requirement that organisations - public and private - inform people if a loss "may give rise to a real risk of serious harm to an individual".

"Serious harm is not limited to identity theft or fraud," the report says. "The harm could include, for example, discrimination, if sensitive medical information was released."

The report indicates that pre-emptive shots have been fired across the bow to defend parts of the business world from inclusion. Banks, for instance, might be regarded as a key justification for mandatory notification, but they have sought exemption.

Boiled down to 10 key issues, the Law Reform Commission recommendations are in the hands of John Faulkner, the Special Minister of State with stewardship of Privacy Act changes. The senator's office will limit itself initially to establishing a national set of privacy principles to resolve discrepancies at state and territory level. It will address privacy matters about credit reporting and health information, and will attempt to update the law to take account of technology change.

Excluded from this first round of legislation is mandatory notification of privacy breaches.

The Law Reform Commission president, Professor David Weisbrot, praises the timetable for approving the first changes to the Privacy Act by early 2010, arguing it will establish important building blocks for further improvement. But Weisbrot wants mandatory notification included as soon as possible.

Companies, he says, must be pushed into proactively protecting customer information.

"I've spoken to Senator Faulkner's office and I said I hope they might rethink that. I think it's something that should be done as soon as practicable."

Unsurprisingly, privacy advocates have also lobbied for this. Nigel Waters, a board member of the Australian Privacy Foundation, says: "We're a bit disappointed. It's the single best thing we could do to get organisations to take privacy seriously."

David Vaille, the executive director of the Cyberspace Law and Policy Centre, fears the issue will be dismissed as too hard, saying: "One problem with having a 2700-page review of privacy, which is fantastically detailed, is that most of it just gets put off for years."

Despite such appeals, Faulkner's office says mandatory notification will fall into a second round of changes. In the meantime, the Privacy Commissioner, Karen Curtis, who supports compulsory notification, has issued voluntary guidelines to help businesses and government departments assess when notification is needed.

"I think mandatory breach notification or some form of it is a natural evolution of our privacy laws," she says. "I think it will be useful to see how our voluntary guide works in practice. That will ensure we get a better law.

"Touch wood, we've been very lucky in Australia. To date there haven't been large-scale breaches," Curtis says before adding a caveat: "That we know of."

Source: The Sun-Herald

This story was found at: <http://www.theage.com.au/articles/2008/11/16/1226770228519.html>