

Exposed: WA Govt IT security bumbles

By [Ry Crozier](#)

Mar 26, 2010 9:32 AM

Laundry list of flaws and stuff-ups.

The Western Australian Auditor-General has revealed he was able to guess passwords for highly privileged database accounts at two of the state's agencies, gaining full access to sensitive information.

Auditor-General Glen Clarke said in a new audit report that changes made using the compromised accounts were undetectable.

The report found another application at a third agency that "allowed users to create single character passwords that did not expire".

Two agencies were also found to store unsecured credit card details - one on a network accessible by any user.

The embarrassing breaches are two in a litany of IT security flaws uncovered at seven of the State's departments and agencies.

They included privileged accounts created by former staff that were still active.

"In two agencies we found numerous network and application user accounts with the highest privileges had been created without approval," Clarke said.

"A number of these accounts belonged to former staff.

"At three of the four agencies [we looked at], we found active user accounts belonging to former staff that allowed access to key applications, the network, and databases."

At two of these agencies there was no monitoring or logging of user access. This makes it impossible to know whether unauthorised access or changes to information had occurred."

There were too many other breaches to describe them all. Some included:

- An agency where the server room did not have air-conditioning, fire systems or basic physical protection of the equipment. "We found several rooms operating at high temperatures," Clarke said.
- An agency where the computer room and agency tea room can be accessed with the same key.
- Two agencies that used generic administrator accounts to access sensitive information from systems. One was unable to provide the required police clearances for staff accessing such information.
- Two agencies that only kept user logs for "several hours" before overwriting them. Then there were the agencies that didn't have logs or didn't look at them period.
- "Excessive numbers of firewall administrators" at two agencies that could change firewall settings. The agencies had no record of changes made.
- Agencies that did not know their patch management systems had stopped working.

Laptops not much better

Part of the report also dealt with lost and stolen laptops and the prevention of information leakage via portable storage devices like flash drives.

On average, 250 laptops were reported stolen every year. Clarke was "reassured" that all agencies required a police report to be filed before they would replace the laptop.

But agencies were exposed for lax practices in making sure information on stolen devices could not be accessed by an unauthorised user.

Three agencies - including the central office of the State's Department of Education - failed basic security tests by giving users full administrative control of their laptops.

Only one agency out of seven - WorkCover - had local firewalls on laptops to protect the device when it connected to a public network.

Four agencies - the Curriculum Council, Department of Water, Department of Commerce and WA Police - had not deployed patches for critical software flaws.

"The Department of Commerce had a security update server configured to manage software patch updates across all laptops, however we found that it had not been functioning properly," Clarke said.

But WA Police won praise for establishing control mechanisms for portable devices including flash drives and for having policies and procedures governing their use. They had also issued encrypted drives to all staff.

Clarke believed his report should be a "wake-up call to Government agencies, particularly those that handle personal and sensitive information".