Video transcript: Cybersecurity of IT Servers

Some background

A successful cyber attack on government agencies can leak sensitive information and disrupt critical infrastructure.

Agencies use IT servers to store, process and share information.

These servers, which can be physical or virtual, provide services to other computers.

Government agencies must make sure their IT servers are secure to:

- help minimise risks of disruptions to operations, and
- prevent unauthorised access to sensitive information.

About this audit

We assessed 10 government departments and Cenitex to:

- see if they know what servers they have, and
- check that the security controls applied on their servers protect them.

What we concluded

We made 2 key findings and concluded that each agency can do more to improve its server security.

Key finding 1

No agency has a complete and accurate server inventory.

We found that the tools agencies use to capture their server information are not effective.

Agencies cannot effectively manage their server security if they don't know what servers they have.

Key finding 2

All agencies can improve the maturity of technical security controls applied to their known servers.

For example, we found that all agencies had servers that were running with unsupported operating systems. This means that these servers do not receive automatic security updates.

This increases agencies' exposure to cyber attacks.

What we recommended

We made 3 recommendations:

- 2 to all agencies about improving tracking of all their IT servers and strengthening the technical security controls on their servers, and
- one to the Department of Government Services about issuing relevant guidance to agencies.

More information

For more information, or to read our full report, go to audit.vic.gov.au