Media contact: Vanessa Sprunt
Mobile: 0427 953 993
Email: vanessa.sprunt@audit.wa.gov.au

24 November 2021

Local government networks and systems at risk due to poor cyber security

The Auditor General today tabled in Parliament the *Cyber Security in Local Government* report.

Through ethical hacking and audit work, we assessed if a sample of 15 local government entities managed cyber security risks and responded to cyber threats effectively.

Auditor General Ms Caroline Spencer said most local governments did not have current and complete cyber security policies and processes to help them manage cyber risks and effectively respond to cyber-threats.

'Our audit included ethical simulated cyber-attacks on local government systems. Concerningly, only 3 entities had their systems configured to detect and block these simulated attacks in a timely manner.

Most entities lacked appropriate cybersecurity incident response plans to guide an effective response to cyber incidents,' Ms Spencer said.

We also found entities were at significant risk of successful phishing attacks despite conducting employee cyber security awareness training.

Ms Spencer said staff at 8 of the 15 local governments clicked on the links in our test phishing emails and, in some cases, submitted their usernames and passwords.

'The lack of controls to prevent phishing emails could potentially expose systems and confidential information to cybercriminals,' Ms Spencer said.

Entities were also not managing system vulnerabilities well, with most at risk due to out-of-date software. Cyber criminals could exploit these weaknesses to gain unauthorised access to LG entity networks and systems.

The report includes recommendations and better practice principles that all public sector entities can adopt to improve their cyber security management.

Report resources

- PDF version
- summary video