Report on a page

Cyber incidents are unwanted or unexpected events that could compromise computer and information systems and business operations. They can cause significant disruption and are happening more often, according to the Australian Cyber Security Centre (ACSC). Across Australia, nearly 94,000 cyber crime reports were made to the ACSC in 2022–23 – a 23 per cent increase in one year. Queensland accounted for 30 per cent of these reports, which is disproportionate to its population size, and one in 8 reports nationally related to state or local government entities. Cyber risks are continuing to evolve, and new technologies such as artificial intelligence increase the risk.

In this report we discuss how prepared Queensland public sector entities, including local governments, are to deal with cyber security incidents. We examined 2 lead agencies with responsibility for guiding cyber security, and we audited 3 other entities with varying levels of resources and capability. We have not named them, to avoid publicly identifying any security vulnerabilities.

The current picture

Since we produced *Managing cyber security risks* (Report 3: 2019–20), the Queensland public sector has invested in building its cyber resilience. The Cyber Security Unit (CSU – Department of Transport and Main Roads) has worked with entities to improve their information security management systems (their policies and procedures for managing sensitive data). The government has made additional investments to provide support, share cyber intelligence, and assist government owned corporations and local governments.

Despite this, public sector entities are not as prepared as they have to be. Just having plans is not enough. They need to test their plans and readiness. They need to identify and address any skills gaps they have for dealing with cyber incidents. Also, some entities do not yet know about the services CSU provides, and CSU does not know which entities most need its help and expertise.

What entities need to do

The entities we audited had plans for managing cyber incidents, but all had room to improve. Their plans were not always well integrated with their risk management strategies, did not incorporate cyber insurance requirements, and were not designed to respond to a wide range of threats. One entity had struggled to integrate its plans due to consistent machinery of government changes (restructures of government functions). Some entities also needed to be clearer on roles and responsibilities and on how to escalate their responses to cyber incidents. Only one entity had tested its incident response plan, and all entities needed to do more to ensure they can effectively communicate in a cyber crisis. Some entities did not have an up-to-date and complete understanding of their critical systems and information assets – an essential starting point for cyber security.

Entities relied heavily on third parties or other government entities when dealing with responses to cyber incidents, and were not always clear on accountability requirements. None had tested how these third parties would perform in a crisis. This means they could not be confident the third parties would be available or have the expertise to deal with a real incident in an effective and timely manner.

What expert and lead agencies need to do

CSU needs to continue working with entities to improve their information security management systems. It also needs to help entities to assess their individual needs, which would assist it in deciding where to focus its support and training. CSU should also start helping entities test their incident response processes. Again, this will benefit CSU, because it will familiarise its external experts with public sector requirements.

The Department of Housing, Local Government, Planning and Public Works needs to ensure councils are aware of the cyber-related skills available through CSU and encourage them to use them.