Queensland Audit Office
Better public services

Managing cyber security risks

(Report 3: 2019–20).
Tabled 1 October 2019.

Welcome

Welcome to our presentation on the performance audit report on managing cyber security risks.

Please note that this is a summary and the full report can be read on our website.

Audit objective

In this audit, we examined whether entities effectively manage their cyber security risks. Our audit included detailed technical testing by specialist security consultants.

We selected three entities for this audit; however, our report provides learnings and recommendations for all entities. We use the term ‘entities’ to refer broadly to all Queensland public sector entities (departments and statutory bodies) and local governments.

Context

Protecting important information assets with secure systems is critical to Queensland’s economic and security interests. The Global Risks Reports produced by the World Economic Forum found that ‘data fraud or threat’ and ‘cyber attacks’ are in the top five most likely global risks.

Media reports show an alarming trend of growing cyber security attacks and corporate espionage targeting government entities, intending to compromise Australia’s economic interest and national security.

We used two better practice frameworks to assess the three entities—the Queensland Government's *Information security policy* (IS18:2018) and the Australian Cyber Security Centre’s ‘Essential Eight’ mitigation strategies to help organisations protect their systems against cyber threats.

Our conclusions

We concluded that the three entities are not managing their cyber security risks as effectively as they could. We identified their key information assets and used these to set targets for our security consultants to test—and they were successful in all three instances. This means the consultants successfully compromised all three entities' ICT environments and gained access to their sensitive or non-public data, demonstrating gaps in the entities’ mitigation strategies.

None of the three entities could demonstrate that they understood the extent to which its information assets were exposed to cyber security risks. All need to conduct a comprehensive assessment to determine which assets are at risk and require further controls to protect. Without this, it is difficult to know whether an entity has implemented the right level of controls to protect its assets.

Entities need to make sure their staff are aware of their responsibilities in managing cyber risks. In particular, we found poor password practices unnecessarily exposed the three entities to attack.

What we recommend

We made 17 recommendations for the benefit of all entities, drawn from the learnings of this audit. These were across the following areas:

- cyber security framework
- information classification
- identifying and assessing cyber security risks
- information asset management
- cyber security risk management strategies
- monitoring and logging.

For more information

For more information on the issues, opportunities and recommendations highlighted in this summary presentation, please see the full report on our website.

Thank you.