Security of critical water infrastructure (Report 19: 2016–17)

Reliable drinking water and wastewater services are essential to all Queenslanders.

Water service providers protect the quality of drinking water by operating treatment plants that remove contaminants. These service providers generally use computer systems to control operations of water treatment plants, and related facilities and assets.

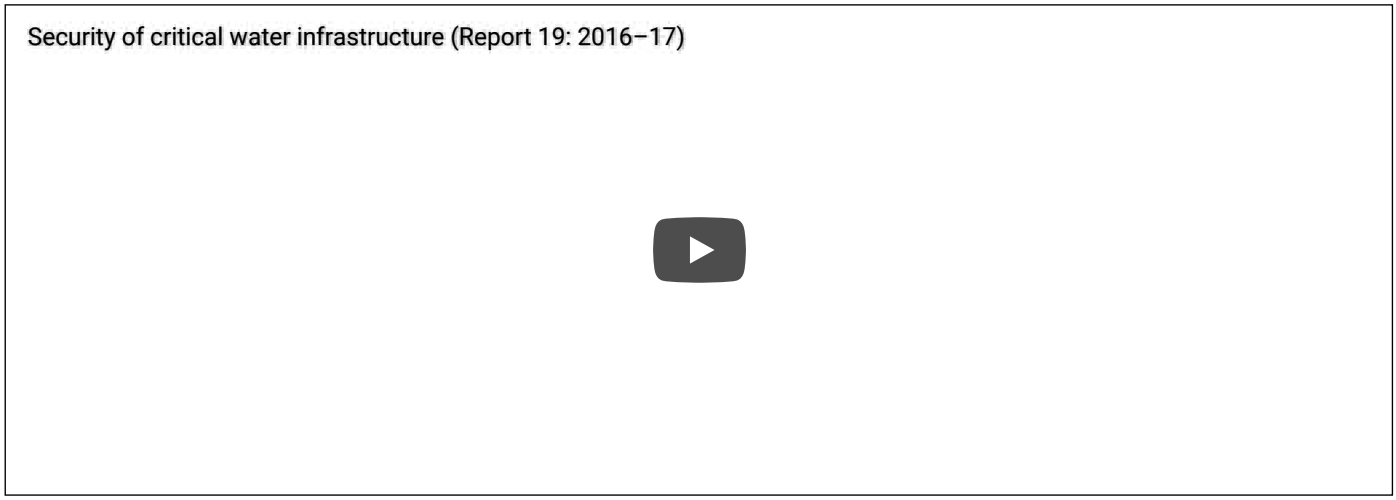
Because of the critical importance of clean drinking water to the community, it is vital that water service providers identify and manage security risks associated with this infrastructure. Failure or security breaches in these control systems can have major consequences for the health of citizens, the environment, and the businesses that rely on these services.

In this audit, we assessed whether a selection of entities responsible for critical water infrastructure have processes in place to protect their water control systems. We carried out our own tests, known as penetration tests, to identify and exploit security vulnerabilities. We also assessed whether these entities could detect the security breaches and restore the systems in the event of an attack.

VIEW REPORT
PDF (2.12 MB)

Watch Presentation

Runtime:
5:19



Recommendations

We recommend that the Department of Energy and Water Supply:

1. integrate information technology risks and cyber threats into the existing risk management framework for drinking water services and in the Queensland water and sewage service provider performance reports. (Chapter 2)
2. facilitate information sharing about adopting standards for securing information technology amongst entities that manage water control systems. (Chapter 2)

We recommend that the entities we audited:

This should include:

- clearly articulating and assigning roles and responsibilities for all parties, including any external service providers in securing the systems
- maintaining a complete and up-to-date list of assets for water control systems and assessing the risk exposure of each asset
- developing and implementing a security plan for water control systems based on risk assessments
- implementing appropriate user access and authentication policies
- using a phased approach to implementing the Australian Government's 'essential eight' security controls based on each entity's risk assessment
- establishing performance indicators for security and periodically testing these controls to monitor the maturity and strength of defences built into the information technology control environment
- improving understanding of how to manage information technology risks and how they relate to other forms of operational risks.

4. establish enterprise-wide incident response plans, business continuity, and disaster recovery processes for information technology. (Chapter 3)

   This should include:

   - testing the capability to respond to wide-scale information technology security incidents either through scenario testing or through desktop exercises
   - training staff to identify, assess, and have a coordinated response to information technology security breaches
   - adopting appropriate business continuity plans that include processes for reporting incidents to stakeholders and building on lessons learned
   - updating and testing information technology disaster recovery and business continuity plans to include processes to recover from a wide-scale information technology security breach
   - considering the impact of multiple system failures on business continuity planning and how entities can operate water and wastewater plants manually, if required.