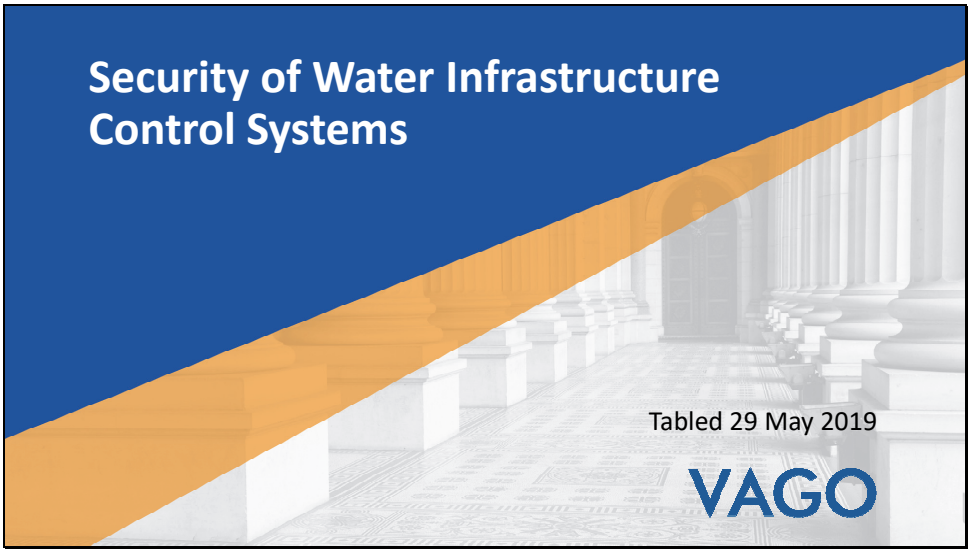
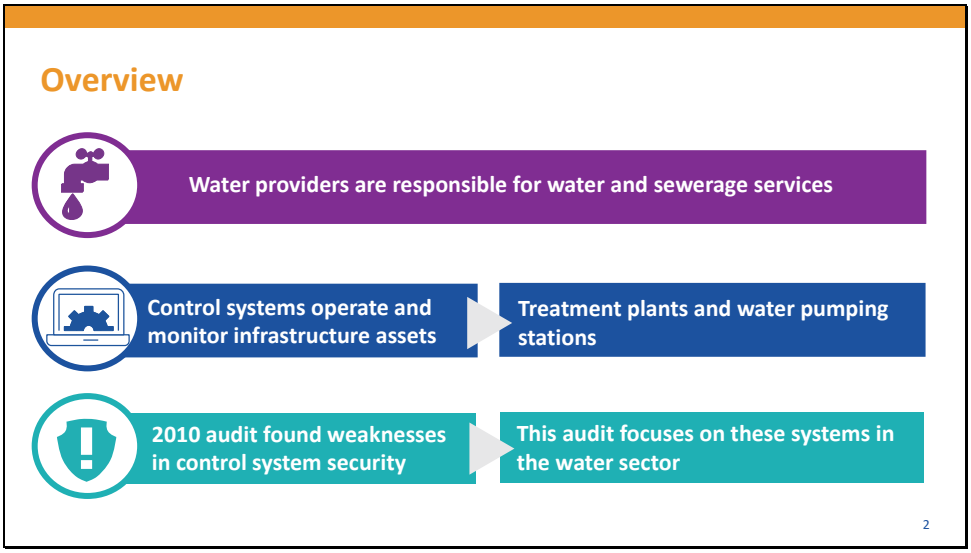
Slide 1



This presentation provides an overview of the Victorian Auditor-General's report Security of Water Infrastructure Control Systems.

Slide 2

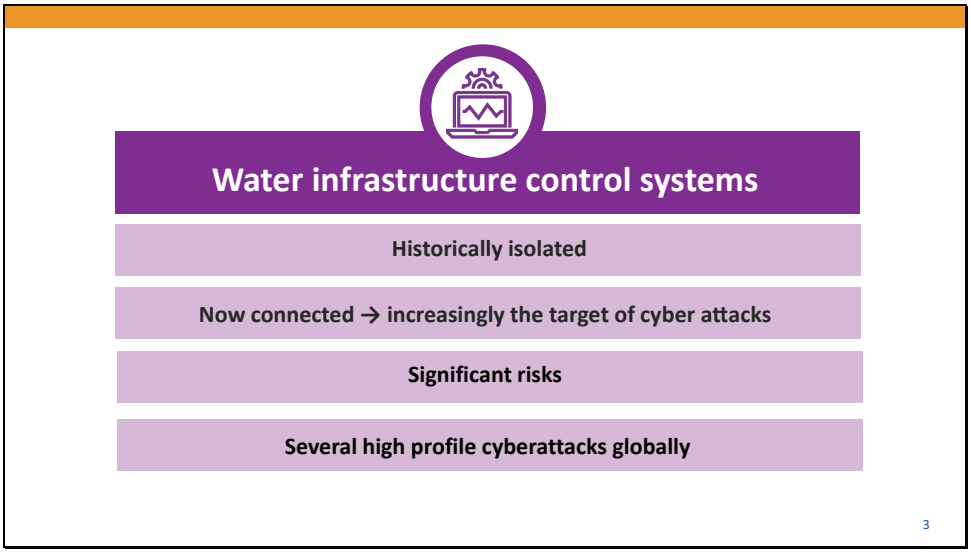


Water providers are responsible for supplying water and sewerage services to Victorians.

Water providers rely on control systems to operate and monitor a portion of their infrastructure assets such as treatment plants and water pumping stations.

Our 2010 audit, *Security of Infrastructure Control Systems for Water and Transport,* noted significant weaknesses in the security of control systems of water and train operators. This audit focuses on control systems in the water sector.

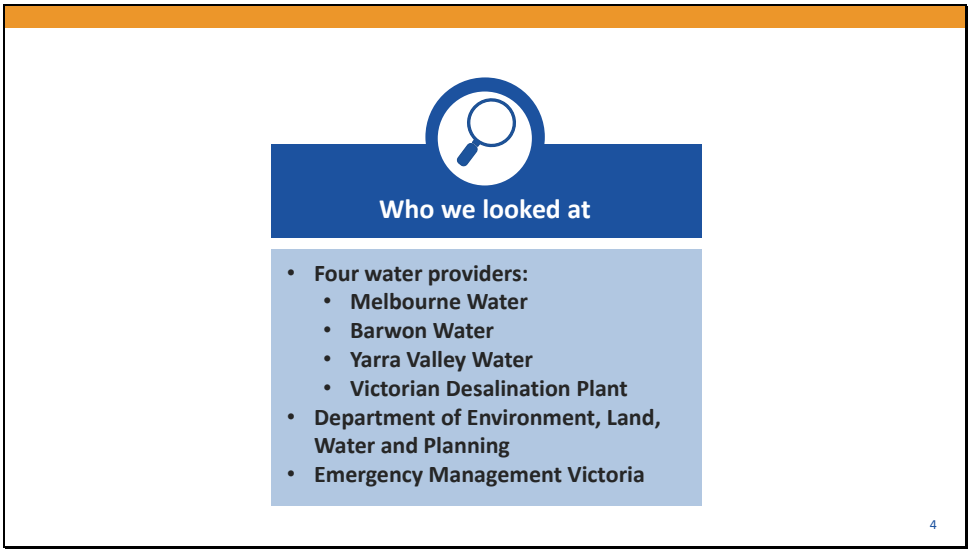
Slide 3



Historically, control systems were isolated from each other, corporate systems and the internet.

Now, they are connected making them increasingly the target of cyberattack.
If successful this poses significant risks to public health and safety, the environment, and the business operations of the entities that use them. There have been several high profile cyberattacks globally on these systems.

Slide 4

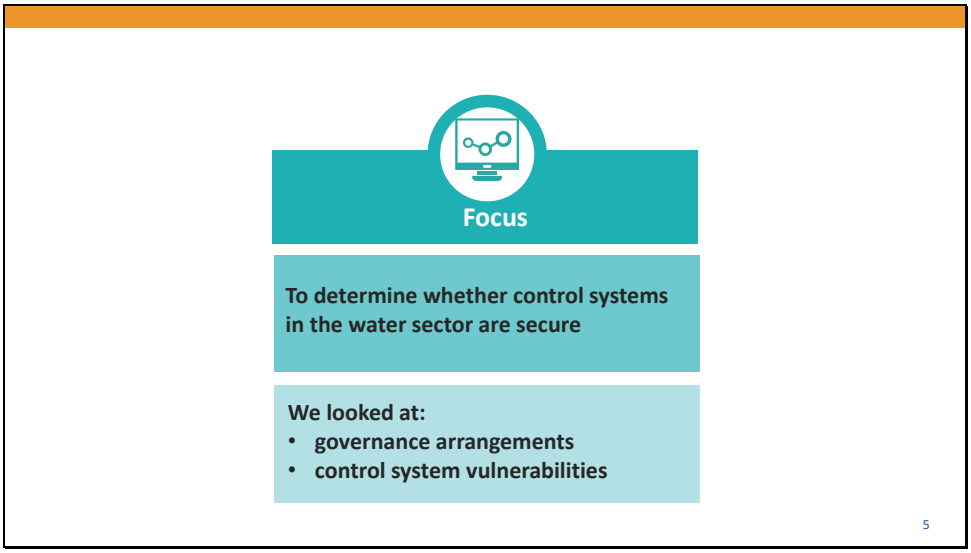


We audited four water providers: Melbourne Water, Barwon Water, Yarra Valley Water and the Victorian Desalination Plant.

We also included the Department of Environment, Land, Water and Planning because it has overall responsibility for the state's water and sewerage services, and water sector resilience.

And we also included Emergency Management Victoria, which leads and coordinates Victoria's emergency management

Slide 5

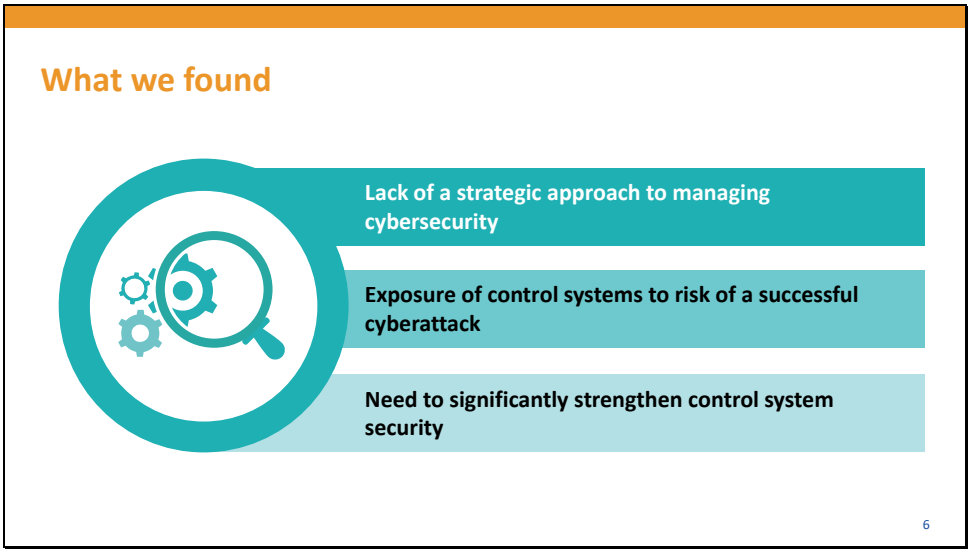


The focus of this audit was to determine whether control systems in the water sector are secure.

We examined the governance arrangements over these systems.

We also undertook a security architecture review, vulnerability assessment and a physical security inspection of a sample of sites.

Slide 6

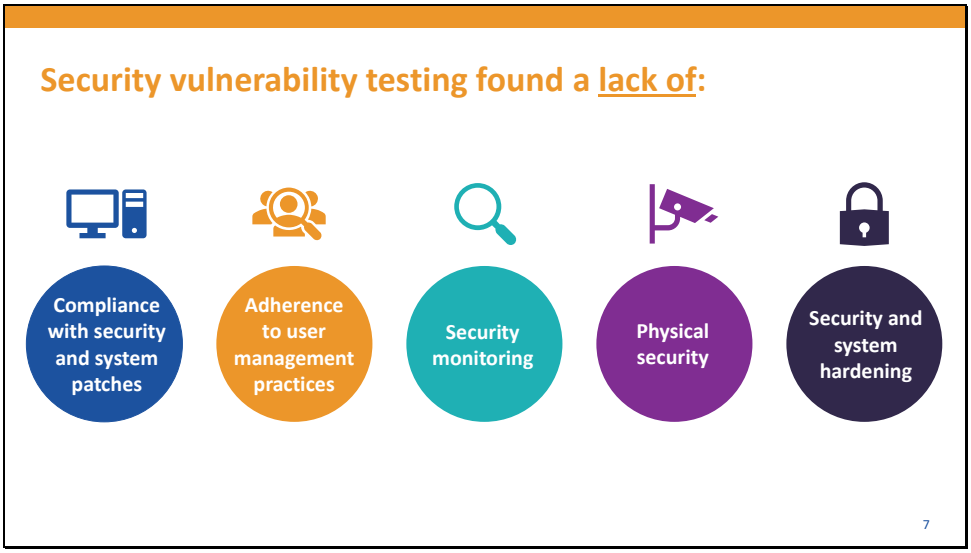


We found that water providers lack a strategic approach to managing cybersecurity risks that integrates their corporate and control system environments and aligns to leading industry security standards for control systems.

This exposes control systems to the risk of a successful cyberattack, particularly by a trusted insider, or an intruder breaching physical security and gaining unauthorised access.

While the audited water providers have actively improved the security of their corporate systems against cyberattacks, evolving threats requires water providers to now increase their focus on assessing and significantly strengthening their control system security.

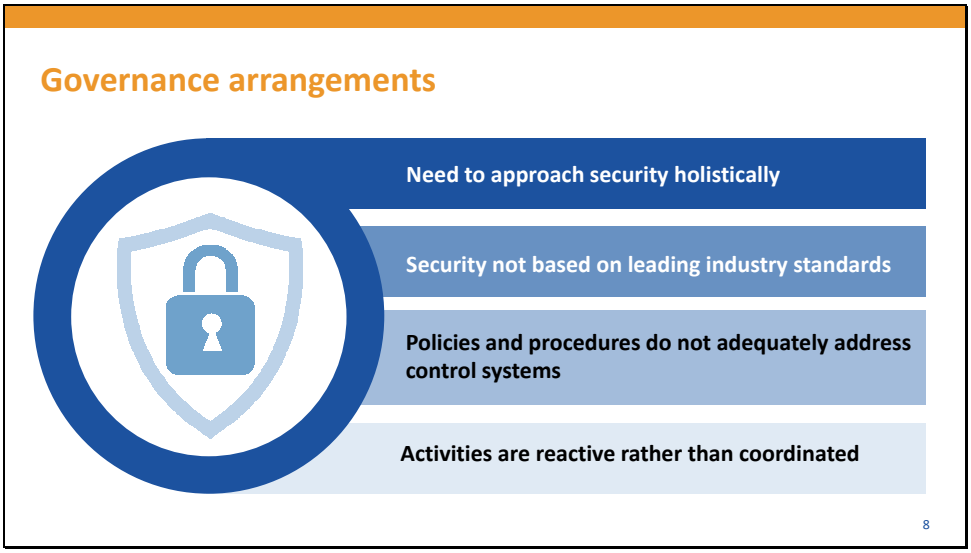
Slide 7



Our vulnerability assessment found water providers did not:

- consistently apply system and security updates
- comply with or enforce user management practices
- monitor systems to identify cyberattacks
- maintain adequate physical security
- minimise opportunities for unauthorised access

Slide 8

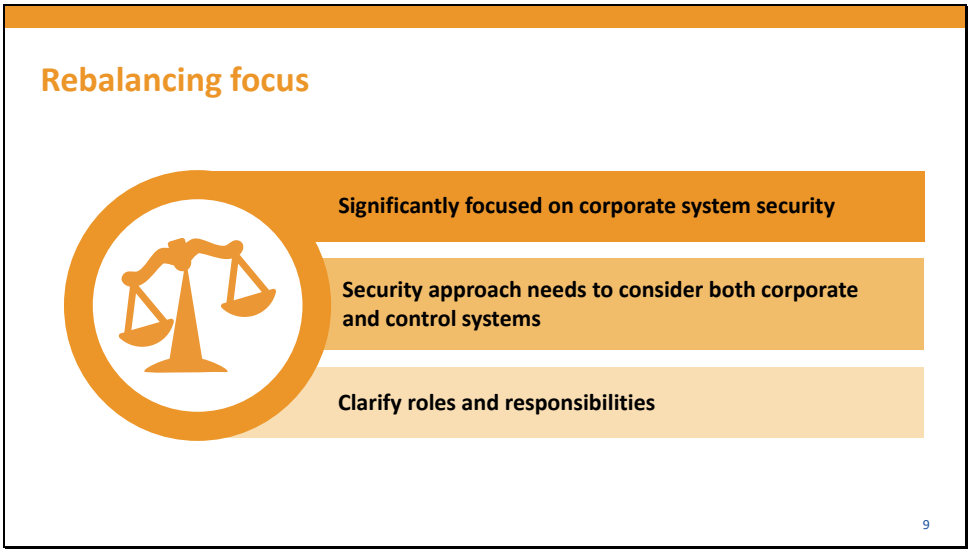


Our review of governance arrangements found water providers need to take a more holistic approach to security.

Currently, water providers have not designed security based on leading industry standards.

Additionally, their security policies and procedures do not adequately address control systems, and security activities are reactive rather than coordinated.

Slide 9



Water providers need to rebalance their security focus. They have invested significantly in securing corporate systems.

However, control systems that deliver critical services are equally as important.

Current security activities have not generally extended to their control systems.

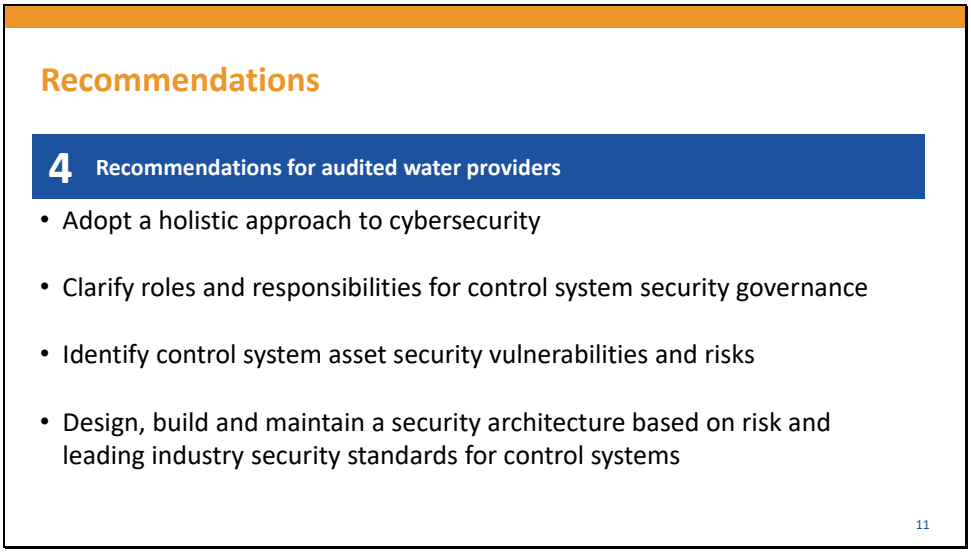
Water providers have not clearly defined roles and responsibilities for the security of these systems.

Slide 10

Water providers' approach to security is not based on a thorough understanding of control system assets, associated vulnerabilities and security risks.

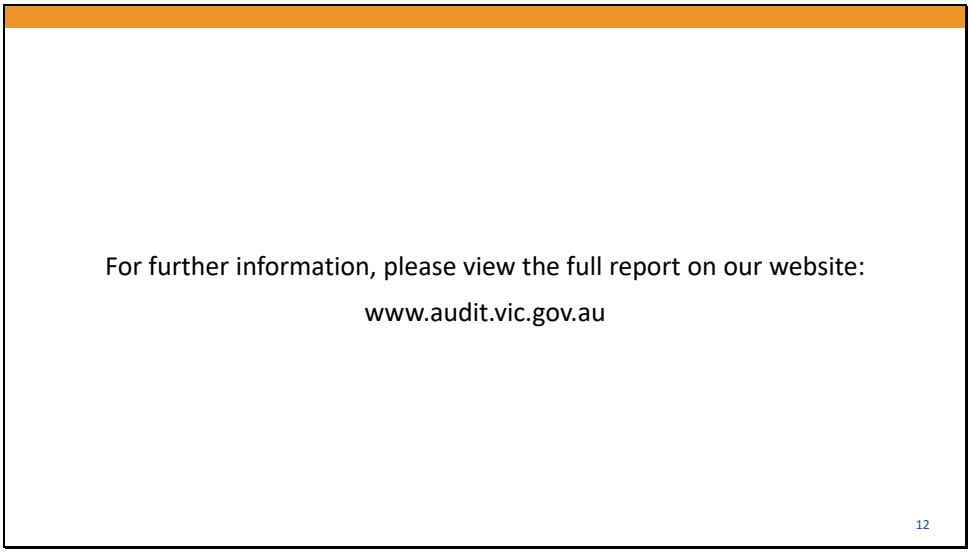
This information is essential for making informed decisions about the appropriate level of security for each part of the business.

Slide 11



We made four recommendations to the water providers to develop a more holistic approach to cybersecurity, based on leading industry security standards.

Slide 12



For further information, please see the full report on our website, at www.audit.vic.gov.au.