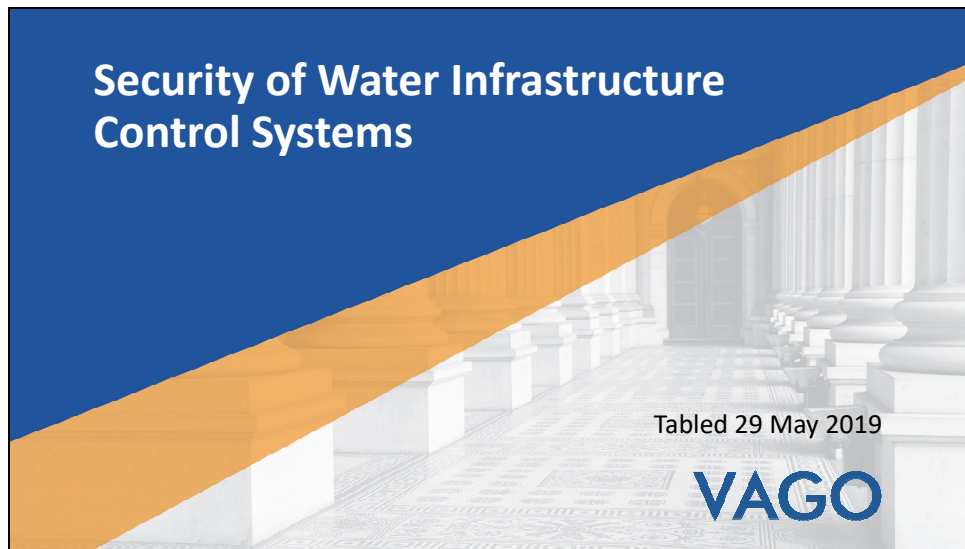
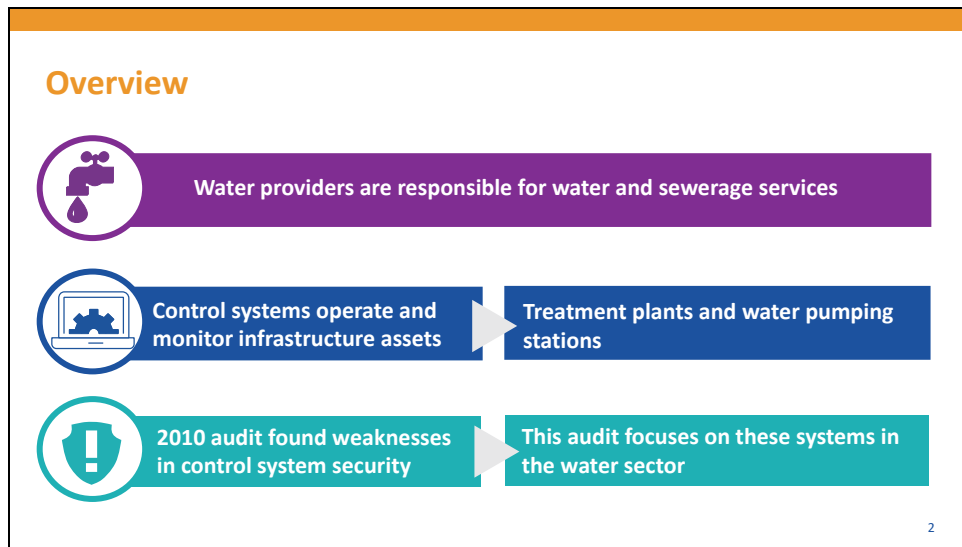


Slide 1



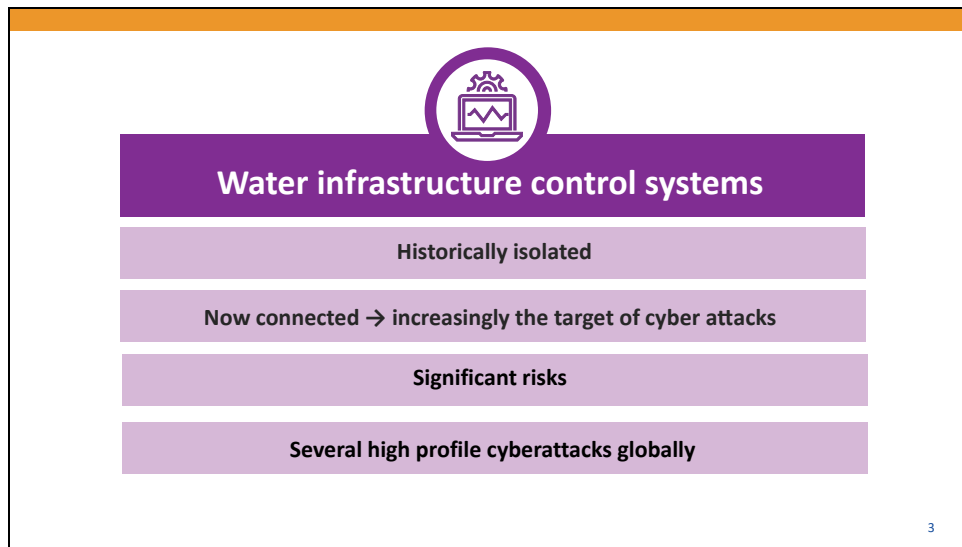
This presentation provides an overview of the Victorian Auditor-General's report Security of Water Infrastructure Control Systems.



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.



The diagram features a central purple circle containing a white icon of a laptop with a gear and a line graph. Below this icon is a dark purple horizontal bar with the text "Water infrastructure control systems" in white. Underneath this bar are four light purple horizontal bars, each containing text in black. The text in the bars, from top to bottom, is: "Historically isolated", "Now connected → increasingly the target of cyber attacks", "Significant risks", and "Several high profile cyberattacks globally". A small number "3" is located in the bottom right corner of the diagram's frame.

Water infrastructure control systems

Historically isolated

Now connected → increasingly the target of cyber attacks

Significant risks

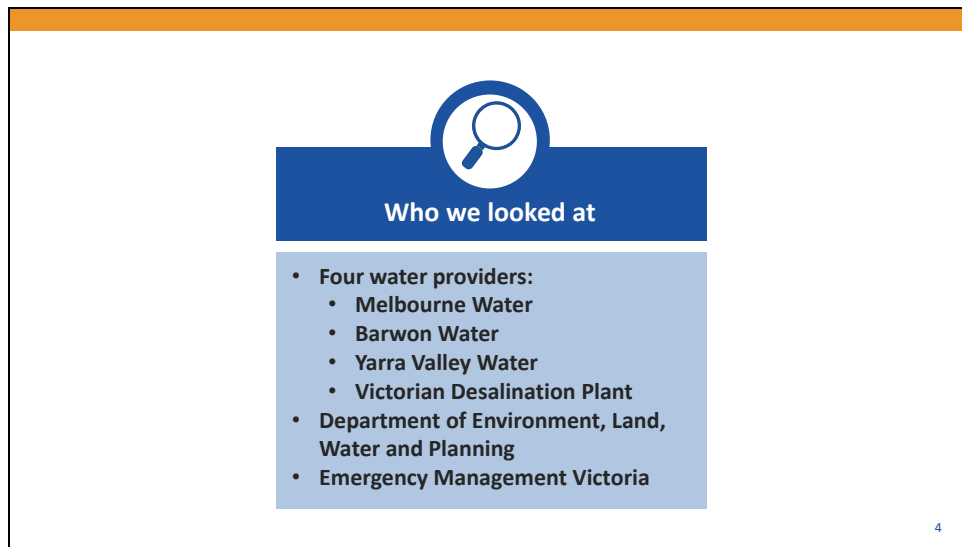
Several high profile cyberattacks globally

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.



Who we looked at

- **Four water providers:**
 - Melbourne Water
 - Barwon Water
 - Yarra Valley Water
 - Victorian Desalination Plant
- Department of Environment, Land, Water and Planning
- Emergency Management Victoria

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

The slide features a teal header bar at the top. Below it, a circular icon with a computer monitor and network lines is centered above a teal box containing the word "Focus". Below this, a light teal box contains the text "To determine whether control systems in the water sector are secure". A final light teal box contains the text "We looked at:" followed by a bulleted list: "governance arrangements" and "control system vulnerabilities". A small number "5" is in the bottom right corner.

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.

What we found



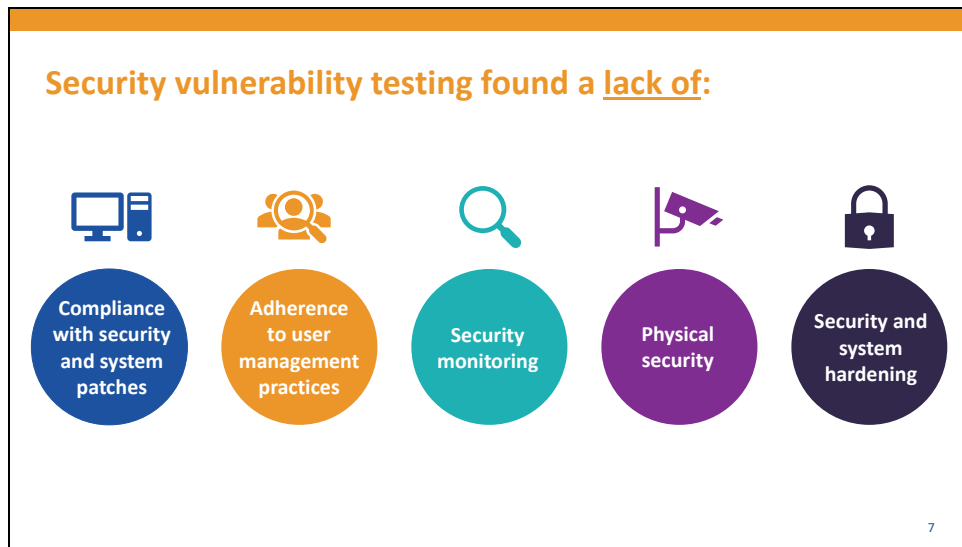
- Lack of a strategic approach to managing cybersecurity**
- Exposure of control systems to risk of a successful cyberattack**
- Need to significantly strengthen control system security**

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.



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

Governance arrangements

- Need to approach security holistically**
- Security not based on leading industry standards**
- Policies and procedures do not adequately address control systems**
- Activities are reactive rather than coordinated**

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.

Rebalancing focus



- Significantly focused on corporate system security**
- Security approach needs to consider both corporate and control systems**
- Clarify roles and responsibilities**

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.

Assessing security risks



Control system assets vulnerabilities and security risks not understood

Essential to inform security decisions

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.

Recommendations

4 Recommendations for audited water providers

- Adopt a holistic approach to cybersecurity
- Clarify roles and responsibilities for control system security governance
- Identify control system asset security vulnerabilities and risks
- Design, build and maintain a security architecture based on risk and leading industry security standards for control systems

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



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

12

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