VAGO

Victorian Auditor-General's Office

Security of Water Infrastructure Control Systems

May 2019

Independent assurance report to Parliament
2018–19: 22

VAGO

Victorian Auditor-General's Office

Security of Water Infrastructure Control Systems

Independent assurance report to Parliament

Ordered to be published

VICTORIAN GOVERNMENT PRINTER
May 2019

PP no 28, Session 2018–19

This report is printed on Monza Recycled paper. Monza Recycled is certified Carbon Neutral by The Carbon Reduction Institute (CRI) in accordance with the global Greenhouse Gas Protocol and ISO 14040 framework. The Lifecycle Analysis for Monza Recycled is cradle to grave including Scopes 1, 2 and 3. It has FSC Mix Certification combined with 99% recycled content.

ISBN 978 1 925678 46 8

VAGO

Victorian Auditor-General's Office

The Hon Shaun Leane MLC
President
Legislative Council
Parliament House
Melbourne

The Hon Colin Brooks MP
Speaker
Legislative Assembly
Parliament House
Melbourne

Dear Presiding Officers

Under the provisions of section 16AB of the *Audit Act 1994*, I transmit my report *Security of Water Infrastructure Control Systems*.

Yours faithfully

Andrew Greaves
Auditor-General

29 May 2019

Contents

Audit overview 7

Conclusion 8
Findings 8
Recommendations 10
Responses to recommendations 10

1 Audit context 11

1.1 Victoria's water sector 12
1.2 Control systems and their use 13
1.3 Securing control systems 13
1.4 Responsibility for security 19
1.5 Better practice cybersecurity standards for control systems 20
1.6 Previous audits 21
1.7 Why this audit is important 22
1.8 What this audit examined and how 22
1.9 Report structure 22

2 Strengthening control system security 23

2.1 Conclusion 23
2.2 Security vulnerabilities 24
2.3 Approaching security holistically 26
2.4 Rebalancing security focus 28
2.5 Comprehensively assessing security risks 29
2.6 Improving response to cybersecurity incidents 31

Appendix A. *Audit Act 1994* section 16—submissions and comments 33

Acronyms and abbreviations

ACSC	Australian Cyber Security Centre
ASD	Australian Signals Directorate
BW	Barwon Water
DELWP	Department of Environment, Land, Water and Planning
DPC	Department of Premier and Cabinet
EM Act	*Emergency Management Act 2013*
EMV	Emergency Management Victoria
IGEM	Inspector-General for Emergency Management
MW	Melbourne Water
NIS Directive	*Network and Information Systems Directive*
NIST	National Institute of Standards and Technology
OVIC	Office of the Victorian Information Commissioner
PDSP	*Protective Data Security Plan*
SCADA	supervisory control and data acquisition
USA	United States of America
VAGO	Victorian Auditor-General's Office
VDP	Victorian Desalination Plant
VPDSF	*Victorian Protective Data Security Framework*
VPDSS	*Victorian Protective Data Security Standards*
Water SRP	*Water Sector Resilience Plan*
YVW	Yarra Valley Water

Audit overview

Throughout this report we refer to infrastructure control systems as '**control systems**', and the water authorities and VDP as '**water providers**'.

Infrastructure control systems, or industrial control systems, are technology used to operate and monitor infrastructure assets. Control systems are critical to delivering the services they support, such as electricity, water, sewerage, gas, transport, and manufacturing. Water providers rely on these systems to monitor or control a portion of their water and sewerage infrastructure assets.

Victoria has 19 state-owned water authorities and the privately operated Victorian Desalination Plant (VDP). Water authorities manage water and sewerage services within their geographic areas, while VDP delivers desalinated seawater under contract with the state government. As critical services, water and sewerage must be safe, reliable, and secure.

Cyberattacks can range from email scams, to physical intrusion, to state-sponsored disruption of computer systems, such as those that manage the electricity grid, water supply or transport networks.

Control systems are increasingly the target of cyberattacks worldwide. This ever-evolving risk is noted in recent audits of these systems in the water and energy sectors undertaken in Queensland and Canada respectively, and an annual review by the United States of America's (USA) Department of Homeland Security.

Our 2010 audit *Security of Infrastructure Control Systems for Water and Transport* found significant weaknesses in control system security, making them vulnerable to cyberattack. We completed a follow-up audit in 2016, *Security of Critical Infrastructure Control Systems for Trains,* and found little improvement in that sector. This audit follows up on the water sector.

Security architecture is the design of security controls within a computer system.

The objective of this audit was to determine whether control systems in the water sector are secure. We reviewed governance arrangements over these systems at four water providers:

- Barwon Water (BW)
- Melbourne Water (MW)
- VDP
- Yarra Valley Water (YVW).

A **vulnerability assessment** finds and ranks weaknesses in a computer system. It informs an organisation of potential threats to its computer systems so it can respond to them.

We also undertook a security architecture review, vulnerability assessment and a physical security inspection of a sample of sites to determine whether any weaknesses in security would put the audited water providers at risk of a successful cyberattack.

We included the Department of Environment, Land, Water and Planning (DELWP) and Emergency Management Victoria (EMV) in the audit. DELWP has overall responsibility for the state's water and sewerage services, and a leadership role in emergency management and water sector resilience. EMV leads and coordinates Victoria's emergency management and plays a key role in critical infrastructure resilience.

Conclusion

Cybersecurity is the defence of computer systems from a cyberattack.

Corporate systems provide applications for customer support, communication, and business processes.

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, the evolving threat landscape requires water providers to now increase their focus on assessing and significantly strengthening their control system security.

Findings

Approaching security holistically

Historically, control systems were isolated from each other, and from corporate systems. Now, water providers use communications technologies to enhance remote control and monitoring capabilities, making it easier for malicious cyberattackers to exploit vulnerabilities to disrupt and damage control systems. Consequently, water providers' focus needs to shift from protecting corporate systems to an integrated security architecture for both systems.

However, water providers have not designed and implemented a security architecture for control systems that is informed by leading industry security standards, to guide a strategic and integrated approach to security.

Security vulnerabilities

Our vulnerability testing highlights the lack of a control system security architecture. We conducted vulnerability testing at each water provider over a three-day period, on a sample of business-critical water and sewerage sites and assets. Risk assessment of the likelihood and impact of each vulnerability occurring, to determine the necessary security measures, was not part of this audit. We also did not review or test water providers' corporate systems.

Our test results show that the audited water providers' current approaches to securing control systems from unauthorised access and use can be significantly improved. We communicated identified vulnerabilities to each water provider. Water providers advise they are committed to improving the security of their control systems and working to address these vulnerabilities.

Monitoring and managing control system security

Water providers have executive sponsors responsible for securing both corporate and control systems. However, they have undertaken limited reporting to their executive on control system security, presenting an opportunity for further attention to this emerging risk area.

Water providers have started to build skills specific to control system security. However, more needs to be done to enhance expertise in this specialised field to effectively manage and improve the security of these systems. In addition, they have not clearly defined and documented roles and responsibilities for the security of these systems.

Comprehensively assessing security risks

Since our 2010 audit, water providers' risk assessments have driven significant investment in enhancing the security of their internet-facing corporate systems and protecting their control systems by separating them from corporate systems. However, control system security at the asset level has not been prioritised.

Water providers have not completed a detailed assessment of the current security risks for control system assets and do not have comprehensive asset information. They have focused their attention on risks to their corporate systems and on high-level control system risks. Therefore, they have not designed or built their control system security based on a thorough and detailed understanding of their assets, vulnerabilities and risks to ensure security measures are proportionate to those risks.

Water providers need a greater understanding of the cybersecurity vulnerabilities and risks across the whole organisation at all levels of their systems to make informed decisions on the appropriate level of security for each part of the business.

Improving response to cybersecurity incidents

The water sector's approach to emergency management has improved, incorporating cybersecurity incidents in emergency exercises. DELWP, as the agency responsible for building water sector resilience, is also leading strong sector engagement and information sharing.

Recommendations

We recommend that Barwon Water, Yarra Valley Water, the Department of Environment, Land, Water and Planning (as the contract manager for the Victorian Desalination Plant), and Melbourne Water:

1. adopt a holistic approach to cybersecurity by integrating security efforts across both the corporate and control system environments (see Section 2.3)
2. clarify roles and responsibilities for control system security governance (see Section 2.4)
3. identify control system asset security vulnerabilities and risks at the detailed level (see Section 2.5)
4. design, build and maintain a security architecture proportionate to risk that is based on leading industry security standards for control systems (see Section 2.5).

We made no recommendations to Emergency Management Victoria.

Responses to recommendations

We consulted with BW, DELWP, EMV—response received from the Department of Justice and Community Safety (DJCS)—MW, VDP and YVW, and we considered their views when reaching our audit conclusions. As required by section 16(3) of the *Audit Act 1994*, we gave a draft copy of this report to those agencies and asked for their submissions or comments. We also provided a copy of the report to the Department of Premier and Cabinet (DPC).

The following is a summary of those responses. The full responses are included in Appendix A.

BW, DELWP, MW and YVW acknowledge the need and are committed to improving cybersecurity of control systems that operate infrastructure in the water sector.

1 Audit context

In recent years, cyberattacks have increased globally and government agencies across Australia are responding to escalating threats. Parliamentarians' emails have been compromised and hospitals' patient data has been hacked with ransoms demanded for its release. The importance of effectively securing computer systems and the information they hold is clear.

Control systems, while unseen to most, play an important part in Victorians' daily lives. They are integral to the supply of critical services such as water, sewerage, electricity, gas, and transport. Water providers rely on control systems to safely and securely supply and distribute clean water and treat and dispose of wastewater.

From the 1960s, control systems began to be used to electronically operate and monitor infrastructure, replacing the onsite personnel who would manually operate equipment. These systems play a key role in improving service efficiency and reliability.

Control systems were originally designed and built as isolated, stand-alone systems. Over time they have been integrated at an operational level, and more recently with corporate systems through incorporating telecommunication services relaying information and data, increased connectivity to the internet to improve remote operation, and cloud-based services to improve a range of support services.

This increased integration improves efficiency and reliability, but makes control systems more vulnerable by increasing the potential entry points to be exploited in a cyberattack. A successful attack poses risks to public health and safety, the environment, and business operations through the manipulation of operational data and service disruptions. It is critical that water providers understand these security vulnerabilities in control systems and have structures and processes to identify, protect, detect, respond to, and recover from security breaches when they occur.

1.1 Victoria's water sector

Roles and responsibilities in the water sector

Victoria's water sector consists of 19 state-owned water authorities and the privately operated VDP. Water authorities provide a range of services to customers within their geographic service areas including water treatment, quality and distribution, and sewerage services. Figure 1A shows the geographic location of Victorian water authorities.

Figure 1A
Map of Victorian water authorities

Source: Water Sector Resilience Plan 2018–19, DELWP.

We assessed three water authorities, BW, MW and YVW, and the privately operated VDP. For the purposes of this report we refer to these organisations as water providers.

MW provides bulk water and sewerage services in metropolitan Melbourne, and manages water courses and major drainage systems in the Port Phillip and Westernport regions.

Three water providers, including YVW, service the Melbourne metropolitan area. The remaining 16 water authorities, including BW, provide water supply and sewerage services to customers in regional and rural Victoria.

The state government contracts VDP to desalinate seawater for delivery to MW and other authorities in quantities ordered by the Minister for Water each year. VDP helps guarantee a reliable, sustainable water supply as it is the only source of water that does not rely on rain. The plant can deliver up to 150 gigalitres of high-quality drinking water a year—one-third of Melbourne's needs—if required. The 2019–20 water order is 125 gigalitres. There are significant contractual incentives to ensure that VDP delivers the volume of water ordered each year.

DELWP has overall responsibility for the state's water resources and sewerage services and an emergency management leadership role in water sector resilience.

EMV leads and coordinates emergency preparedness, response and recovery across the emergency management sector, including the water sector. EMV maintains the critical infrastructure register for the state and plays a key role in the state's approach to critical infrastructure resilience, including the water sector.

1.2 Control systems and their use

Water providers' use of control systems

Control systems are the technology used to operate and monitor infrastructure assets. These systems include the hardware and software that controls equipment and the information technology that gathers data. It includes supervisory control and data acquisition (SCADA) systems, process control systems, and other devices such as programmable logic controllers.

Water providers use control systems to operate and monitor water infrastructure such as water and sewerage networks and treatment plants. One of the benefits of control systems is that they allow water providers to manage sites remotely, reducing the need to have onsite staff at all the sites where their infrastructure is located.

1.3 Securing control systems

What is cybersecurity?

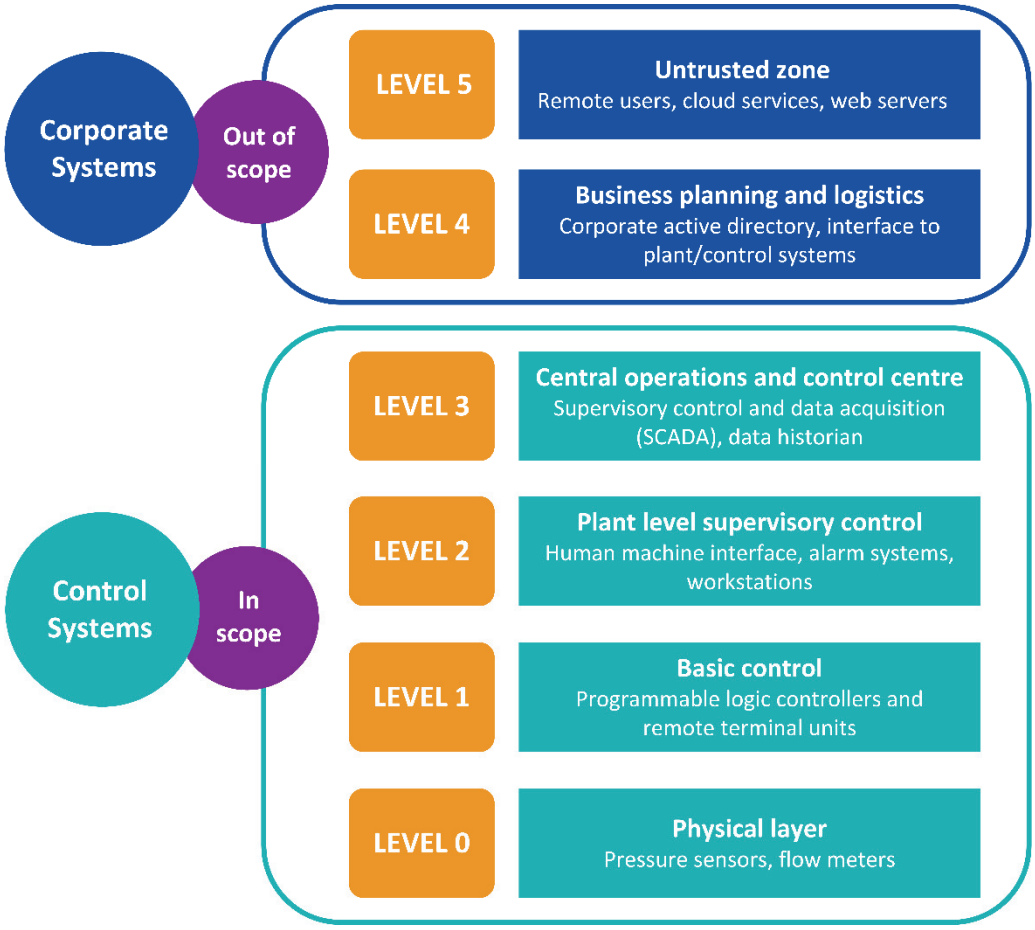
Cybersecurity is the practice of protecting computer systems from unauthorised access, cyberattacks, or damage. Cyberattacks can be internal or external and are usually aimed at accessing, changing or deleting sensitive information or disrupting business processes and services. Implementing effective cybersecurity measures is becoming more challenging as technology evolves and cyberattackers become more innovative and sophisticated.

Control systems are becoming more connected to corporate systems and the internet. Security approaches are necessary equally across both environments because there are many potential entry points to these systems that cyberattackers can exploit. As technology becomes more affordable and with the advent of the Internet of Things—electronic devices with embedded technology allowing connection to the internet—everything is more connected.

Addressing control system security poses different challenges due to the specialised hardware and software, and the need to maintain reliable, available, and supportable services.

A useful way to distinguish and understand these two environments is to examine the computer systems and activities that occur in each of them. Figure 1B illustrates the difference between the corporate systems environment (Levels 4 and 5) and the control system environment (Levels 0 to 3). Corporate systems were out of scope of this audit.

Figure 1B
Corporate and control system hierarchy



Source: VAGO, based on the Purdue Model for Control System Hierarchy.

How are systems best secured

Effective cybersecurity requires a coordinated and balanced approach across the system hierarchy including the domains of security—personnel, physical, computer systems, and information management. This approach provides security coverage across both the corporate and control system environments to comprehensively manage security vulnerabilities.

There are currently no Victorian or Australian security standards specific to control systems. In the USA, the National Institute of Standards and Technology (NIST) developed a *Framework for Improving Critical Infrastructure Cybersecurity* and a guide to control system security, *NIST Special publication 800-82*. The framework and guide offer a risk-based approach to managing cybersecurity for critical service providers, and are leading better practice guidances endorsed by industry.

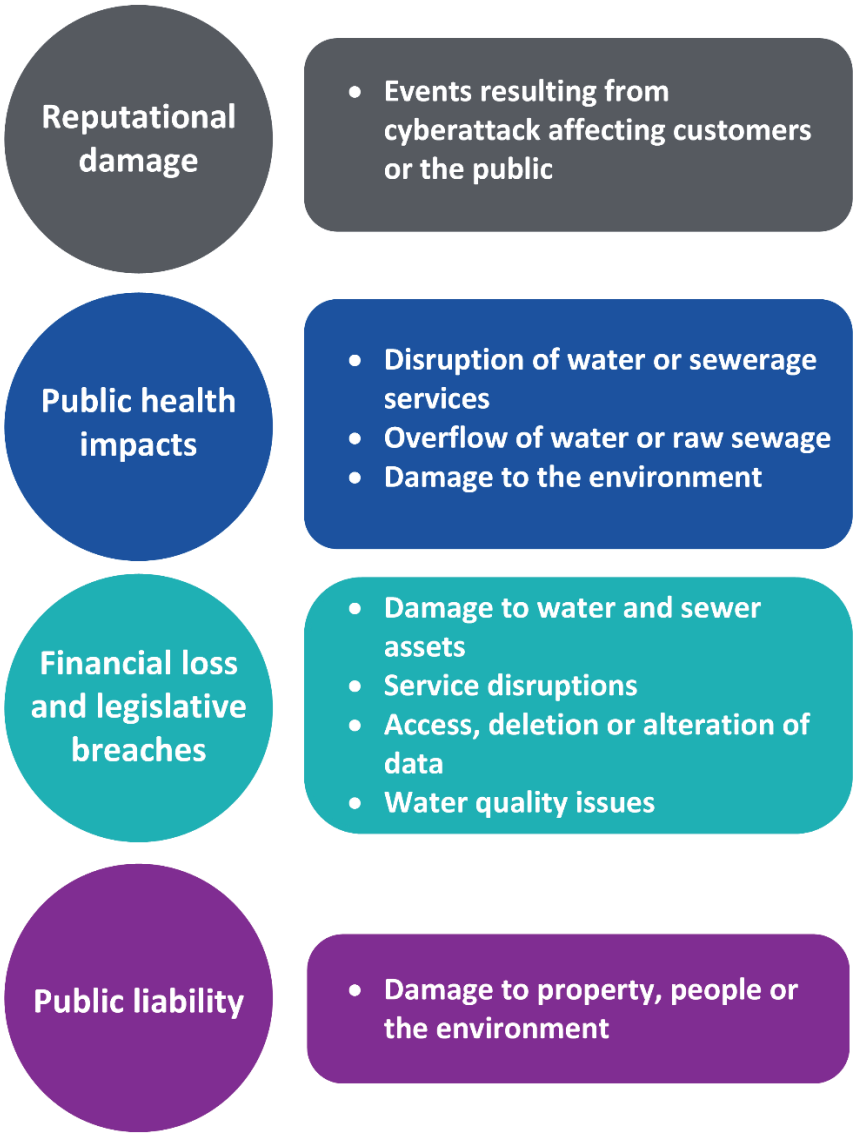
At the core of this framework are five functions that guide cybersecurity risk management:

- **Identify**—the resources that support critical business services, their assets, and security risks.
- **Protect**—develop and implement safeguards to ensure delivery of services. This includes access control, awareness and training and data security.
- **Detect**—develop and implement activities to monitor and detect a cybersecurity incident.
- **Respond**—develop and implement activities to respond to a cybersecurity incident.
- **Recover**—develop and implement activities to maintain plans for resilience and to restore services affected by a cybersecurity incident.

What if control systems are not secure?

Cybersecurity threats to water control systems can pose significant risks to public health and safety, the environment, and business operations. Figure 1C describes the impacts on water providers, critical services and the public of a potential cyberattack on water control systems.

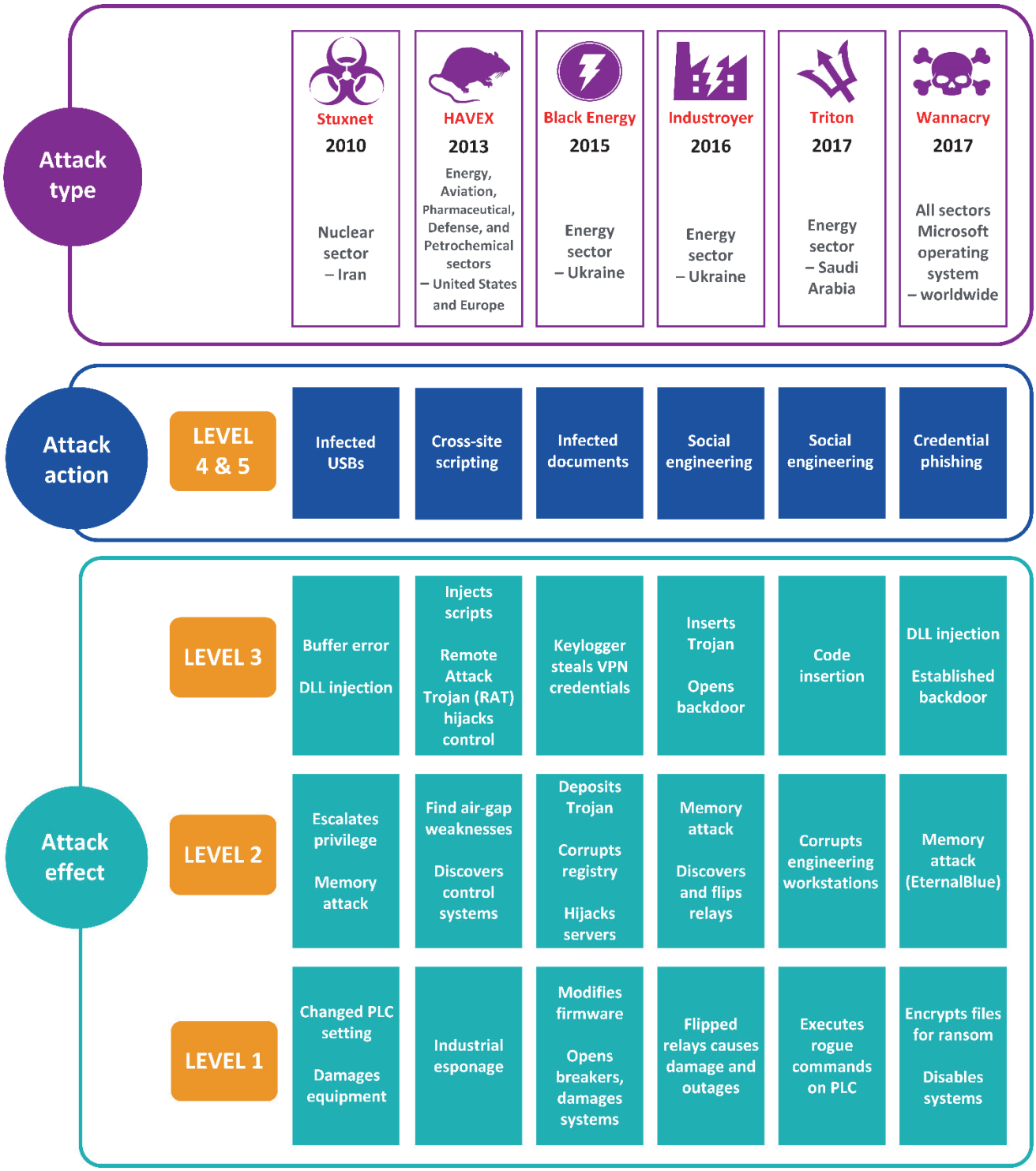
Figure 1C
Potential impacts of a cyberattack on water control systems



Source: VAGO.

Figure 1D outlines past cyberattacks on control systems, how the attack was committed, and the impact the attack had on control systems.

Figure 1D
Cyberattacks and risks to control systems



Note: PLC—programmable logic controller, USB—universal serial bus, VPN—virtual private network, DLL—dynamic link library.
Source: VAGO, based on Schneider Electric, *Protect critical water and waste water infrastructure*, 2016.

1.4 Responsibility for security

Control system operators

According to the Australian national guidelines for protecting critical infrastructure, water providers as operators and VDP as custodians of critical infrastructure are responsible and accountable for protecting this infrastructure, including the control systems that support them.

In addition, under the *Victorian Protective Data Security Framework* (VPDSF) the water providers as control system operators are required to assess and report their management of information and data security risks.

The role of government in cybersecurity

Federal efforts to improve cybersecurity

The Australian Cyber Security Centre (ACSC), part of the Australian Signals Directorate (ASD), leads the Australian Government's efforts to improve cybersecurity. ACSC monitors and assesses the national cyber risk environment, provides guidance, and investigates cybersecurity incidents. The Joint Cyber Security Centre represents ACSC in Victoria. All water providers subscribe to ACSC updates and are members of security forums.

Victoria's role in cybersecurity

In 2017, the Victorian Government released the *Cyber Security Strategy* to improve agencies' detection and prevention capabilities, and responses to cyberattacks. The strategy acknowledges that the compromise of control systems can result in a major disruption to critical services to the community. Key to the strategy is a whole-of-government approach to information security, including the creation of cyber services, capabilities, reporting, executive engagement, and information dissemination.

The strategy notes that DPC, in consultation with EMV, is developing clearer cyber emergency governance arrangements. It also acknowledges that the compromise of control systems, including SCADA systems, can result in a major service disruption to the community. The strategy calls for the establishment of a SCADA cybersecurity working group to develop and implement a cybersecurity program to build readiness and capability. This group was established in May 2017 but the group determined in 2018 that SCADA matters would be better dealt with by the eight Sector Resilience Networks, established under Victoria's *Critical Infrastructure Resilience Strategy*. The Water Sector Resilience Network is a DELWP-led forum for the water sector to collaborate on resilience matters by sharing information and experiences.

New mandatory information and data security reporting

In June 2016, the government introduced the VPDSF under the *Privacy and Data Protection Act 2014.* The VPDSF requires agencies, including water authorities, to manage and report on information and data security.

Government agencies, including water authorities, have mandatory requirements under the VPDSF to:

- undertake a detailed security risk profile assessment
- complete a *Victorian Protective Data Security Standards* (VPDSS) self-assessment
- develop a detailed *Protective Data Security Plan* (PDSP)
- submit a PDSP including an annual attestation to the Office of the Victorian Information Commissioner (OVIC)
- review the PDSP at least every two years, or sooner if there is significant organisational change.

All water authorities submitted their first required PDSP on 31 August 2018. OVIC advised that it expects these reports to include security programs and practices which may include reference to control systems.

The role of government in critical infrastructure

Managing Australia's security risks

Federal legislation designed to identify critical infrastructure assets to manage Australia's security risks came into effect in July 2018. The legislation includes a range of obligations and powers relating to critical infrastructure assets, including the water sector. The Critical Infrastructure Centre is responsible for working with infrastructure owners and operators to identify assets and manage risks of coercion, espionage and sabotage. Reporting requirements commenced on 1 January 2019.

Critical infrastructure in Victoria

In July 2015, the state's emergency risk management arrangements for critical infrastructure resilience came into effect, including:

- Part 7A of the *Emergency Management Act 2013* (EM Act)
- Victoria's *Critical Infrastructure Resilience Strategy,* which drives the requirement for a *Water Sector Resilience Plan* (Water SRP) developed by DELWP in conjunction with operators
- the Water Sector Resilience Network.

These arrangements require critical service providers to assess the importance of their infrastructure and identify interdependent assets, including computer systems needed to continue the delivery of these services. Control systems are an example of an interdependent computer system that service providers should assess.

DELWP undertakes a broader role in leading the planning for water sector resilience through annual development of a Water SRP. The Water SRP includes information on the key emergency risks for the sector and critical dependencies and identifies resilience improvement initiatives for the coming year. The 2018–19 Water SRP identified cybersecurity as a high-risk area for the water sector and includes the following resilience improvement initiatives designed to improve cybersecurity resilience:

- focusing on cybersecurity risks in Water Sector Resilience Network meetings and activities
- reviewing water sector emergency response plans, protocols and guidance
- exercising emergency response plans by DELWP and water agencies.

The Inspector-General for Emergency Management (IGEM) monitors, reviews and assesses critical infrastructure resilience at a system level. IGEM's 2017 report, *Critical Infrastructure Resilience—Implementation Progress Report*, states that it was satisfied that government organisations work collaboratively with their sectors in implementing activities in line with the state's arrangements. The report notes that the water sector, led by DELWP, is engaging with emerging issues such as cybersecurity, and has run an exercise to test emergency management processes and capabilities based on a cybersecurity scenario.

1.5 Better practice cybersecurity standards for control systems

Adopting international standards to improve control system security

Neither Victoria nor Australia have formally adopted security standards specific to control systems. Other states and countries have developed and/or adopted security standards specific to control systems. Examples include:

- Transport for NSW adopted *IEC 62443—Security for Industrial Automation and Control Systems* as a mandatory standard effective July 2018. IEC 62443 is the global standard for the security of control systems and helps organisations reduce the risk of exposing these systems to cyberattacks.
- In 2016, the European Union developed the *Network and Information Systems Directive* (NIS Directive) to improve the security and resilience of control systems for critical services across all member countries. The NIS Directive requires the adoption of IEC 62443, and the United Kingdom has implemented this.

Victorian Protective Data Security Standards

The recent introduction of the VPDSS has driven water providers to assess their information security arrangements. The VPDSS were designed to uplift Victorian government agencies' information security practices for all systems, based on the value of the information they hold or systems they operate.

OVIC provides agencies with flexibility in implementing the standards. A list of high-level security measures called the VPDSS Elements have been derived from the 'control reference' material that is listed within the VPDSS. These provide a focus point for organisations to then define the controls applicable to their specific environment. The standards instruct agencies to refer to relevant sections of the following guidelines to assess and develop their security measures:

Victorian and Australian guidance:

- *Victorian Protective Data Security Framework*
- *Australian Government Information Security Manual*
- *Victorian Government Risk Management Framework*
- *HB 167:2006 Security risk management*
- *AS ISO/IEC 27001/2:2013 Information Technology—Security Techniques*

International guidance:

- *ISO 31000:2009 Risk Management: Principles and guidelines.*

Other sources of guidance

Good practice dictates control system operators should keep pace with technical developments in these systems. New developments mean operators need to continually assess and adjust their security measures at all levels of these systems. Some operators supplement their approach to securing control systems with Australian guidance and leading industry guidance, including:

Essential Eight are prioritised mitigation strategies developed by the ASD to assist government agencies in protecting their computer systems against a range of cybersecurity threats.

Australian guidance:

- ASD—*Essential Eight Explained*

International guidance:

- *IEC 62443—Security for Industrial Automation and Control Systems*
- Sherwood Applied Business Security Architecture
- NIST—*Framework for Improving Critical Infrastructure Cybersecurity* and a guide to control system security, *NIST Special publication 800-82.*

1.6 Previous audits

In 2010, our audit *Security of Infrastructure Control Systems for Water and Transport* noted significant weaknesses in the security of control systems of water and train operators. Control systems were not adequately secure, and appropriate governance arrangements were not in place to provide assurance to management about the security of these systems.

Our 2016 audit *Security of Critical Infrastructure Control Systems for Trains* found significant weaknesses remained for trains and limited improvement since our 2010 audit.

1.7 Why this audit is important

This audit aims to provide assurance on the adequacy of actions undertaken to enhance the security of control systems for the water sector.

The audit examined the management of critical water infrastructure at the portfolio and water provider level to understand the operation of each provider's business processes and the security frameworks they use over control systems. We assessed the effectiveness of the security processes for control systems used to operate and monitor important water infrastructure.

The security of these assets is critical for the efficient and reliable delivery of quality water and sewerage services across the state.

1.8 What this audit examined and how

Our objective for this audit was to determine whether control systems in the water sector are secure.

We examined the governance arrangements in place to manage security threats and events involving control systems and whether the security measures over these systems ensure operational stability, resilience and consistency.

We engaged technical specialists to undertake a security architecture review, vulnerability assessment and a physical security inspection of the infrastructure control system environment within each of the water providers.

We conducted vulnerability testing at each water provider over a three-day period, on a sample of business-critical water and sewerage sites and assets. Their corporate systems were not subject to review or testing. Risk assessment of the likelihood and impact of each vulnerability occurring, to determine the necessary security measures, was not part of this audit.

We conducted our audit in accordance with section 15 of the *Audit Act 1994* and ASAE 3500 *Performance Engagements*. We complied with the independence and other relevant ethical requirements related to assurance engagements. The cost of this audit was $640 000.

1.9 Report structure

Part 2 examines the outcomes of our assessment of the security of control systems.

2 Strengthening control system security

Effective cybersecurity management by water providers requires a risk-based approach to security, executive sponsorship, appropriately skilled security staff, and continual review and testing of the strength of security measures. The approach should be guided by leading industry security standards to ensure the security measures chosen are effective.

Control systems are increasingly the target of cyberattacks worldwide. This ever-evolving risk is noted in recent audits of these systems in the water and energy sectors undertaken in Queensland and Canada respectively. These systems were previously considered to be low-risk, but this is no longer the case. For this reason, we reviewed the governance arrangements for control systems at four water providers and tested their security measures for these systems.

2.1 Conclusion

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.

Since our audit in 2010, water providers have actively invested in improving the security of their corporate systems against cyberattacks and attempted to protect control systems by separating them from corporate systems. However, they have not designed and built security measures for their control system environments based on a comprehensive understanding of security risks at the asset level. The results of our vulnerability tests demonstrate that significant weaknesses exist in the current approach to securing control systems.

2.2 Security vulnerabilities

Review of governance arrangements

We reviewed water providers' governance arrangements over control systems, including assessments of:

- established roles, responsibilities, and sponsorship of control systems
- policies and procedures that make up their security framework
- detailed vulnerability and risk assessments of control system assets
- coordination of response and recovery plans
- action taken on previous recommendations and improvement processes.

Testing control system security

We completed a security architecture review, vulnerability assessment, and a physical security inspection of the control system environments at each water provider. The corporate system environments were not subject to review or testing, other than assessing information flows and security controls between the two system environments. Risk assessment of the likelihood and impact of each vulnerability occurring, to determine the necessary security measures, was not part of this work.

Testing approach

Our approach to vulnerability testing was designed to minimise the impact on control system performance and safety. We adopted a grey box testing approach to identify system vulnerabilities, which was planned, controlled, incremental, and approved in advance by water providers. This means we had some knowledge of the network design of their computer systems, so we could develop the focus of each test.

We consulted with water providers in developing test plans. Plans were customised and included a sample of business-critical water and sewerage treatment and pumping sites. This enabled us to test a range of different control system assets, hardware and software, at each site.

We conducted internal testing within the water providers' system environments and an external physical security inspection.

Test results and key vulnerabilities

Our vulnerability testing of the security of water providers' control systems, against leading industry standards, show vulnerability to an internal cyberattack or an outsider breaching physical security.

We identified vulnerabilities in common with international assessments of control systems. The USA Department of Homeland Security's *ICS-CERT Annual Assessment Report FY 2016* assessed 130 control systems across a range of sectors, 75 per cent representing energy, transport, government and water. The six most common vulnerabilities and their risks identified in the USA report compared with the audited water providers' vulnerabilities are shown in Figure 2A.

Figure 2A
Common control system vulnerabilities compared to audited water providers' vulnerabilities

Top six vulnerabilities	Risks	Water sector key vulnerabilities
1. Boundary protection	Undetected, unauthorised access Weak boundaries between corporate and control systems	**Lack of compliance with security and system patches** Not consistently applying application, operating system or security updates
2. Least functionality	Increased opportunity for malicious access to control systems Rogue internal access	**Lack of security and system hardening** Failure to minimise security risks in control systems which could allow unauthorised access
3. Identification and authentication	Lack of accountability or traceability for user actions if an account is compromised	See vulnerabilities 5 and 6 below
4. Physical access control	Unauthorised physical access to field equipment and locations provides increased opportunity to: • maliciously modify, delete or copy device programs or firmware • access control systems • steal or vandalise cyber assets • add rogue devices	**Lack of physical security** A lack of physical security policy and procedures for the control systems to guide the use of mobile devices, access management and controls and device installation and removals processes
5. Audit review, analysis and reporting	Without formalised review and validation of logs, unauthorised users, applications or other unauthorised events may operate in the control system network undetected	**Lack of physical security monitoring** Lack of security monitoring meaning cyberattacks may not be identified, causing disruption to control systems
6. Authenticator management	• Compromised unsecured password communications • Password compromise could allow trusted unauthorised access to systems	**Lack of adherence to consistent user management practices** Failure of staff to comply with and enforce user management practices

Source: VAGO using The Department of Homeland Security, USA, *ICS-CERT Annual Assessment Report FY 2016.*

We have not included the detailed test results in this report as this may expose water providers to cyberattack. They have received individual reports detailing:

- test results and findings
- vulnerabilities that may expose their control systems to unauthorised access and use
- recommendations to take a more strategic approach to control system security and remediate weaknesses.

The individual reports provide a vulnerability assessment of a sample of sites and assets, which do not include a risk assessment. We expect each water provider to undertake the latter based on their specific risk-appetite.

Water providers advise that they are committed to prioritising the strategic recommendations and addressing weaknesses identified by their risk assessment.

Noting that our vulnerability testing was limited in scope, it is a good starting point for water providers to undertake further work to assess all assets for remaining sites and complete a comprehensive risk assessment.

2.3 Approaching security holistically

Shortcomings in security frameworks

Water providers have a framework of policies and procedures to guide the security of their corporate systems. However, these documents lack a targeted and detailed approach to managing the security of their control systems. For example, security procedures for installing control system equipment should include the security measures to be applied at installation. Further, existing equipment in the control system environment should be audited and the necessary security settings applied to ensure they are appropriately protected from unauthorised access.

Three water providers have reviewed their security frameworks in the past year:

- One has included references to control systems and now needs to further align corporate and control system frameworks.
- One recognised that its newly developed cybersecurity strategy did not adequately consider control system security and has approval to develop a comprehensive approach for these systems within the existing strategy.
- One brought together existing control system procedures in a single enterprise security framework recognising an effective approach must encompass the domains of security—information, personnel, computer systems and physical. They are now consolidating these procedures and need to consider how they work together to provide sufficient security coverage.

Developing an integrated approach

Water providers deploy reactive solutions in response to detected security issues, rather than designing security in a way that coordinates activities across all systems, addressing the root cause of security weaknesses. Figure 2B illustrates the impact of not monitoring control systems for unauthorised devices, which is one of the risks faced by control systems operators and highlights the importance of security design.

Figure 2B
Rogue devices

A rogue device is an unauthorised device attached to a computer system that poses a security risk.

An individual could exploit vulnerabilities in a control system by connecting a rogue device to an unprotected access point and gaining unauthorised access. Control system operators should periodically scan for, detect and remove unauthorised devices connected to their systems. This was not the case at one water provider. Without these documented and approved procedures, a rogue device added to the environment can go undetected.

Source: VAGO.

Changing the approach to security

To minimise their vulnerabilities and mitigate risks, water providers need to change their current approach to security and align with leading industry security standards for control systems. None of the water providers have designed and built a security architecture to guide a thorough and integrated approach to security of these systems.

Better practice guidance

Our 2010 audit recommended that water providers rigorously review the security of their control systems against the relevant state and international security standards and implement improvements. They are informally looking at Australian and international security standards to guide their security approach for corporate systems, such as NIST, and are actively implementing the ASD Essential Eight. One provider is periodically self-assessing and tracking their maturity against NIST. Further, two have applied the ASD Essential Eight to both their corporate and control systems.

OVIC has subsequently released VPDSS, which refers to local, national and international better practice guidance for information and data security. However, as there are no Australian security standards specific to control systems, water providers should seek guidance for securing these systems from international standards. Specific standards advocate for a more sophisticated approach to designing control system security, such as IEC 62443 and NIST 800 82. The IEC 62443 standard focuses on the design of a security architecture. Only one water provider has referred to these standards in a proposed security strategy for control systems.

It is at the discretion of the water provider to determine the use of a standard commensurate to their size and the criticality of service delivery. Regardless of the standard used, it is important that they use a respected and trusted leading industry standard for control systems to guide the design, implementation, review and improvement of control system security.

Responding to reviews and tests

Water providers take findings and recommendations from reviews, audits, and tests conducted on their corporate environments, and address each item separately. They log individual items into a system for tracking action, assessing vulnerabilities and risks and developing a treatment plan to resolve the security weakness if required. This occurs in isolation from a security architecture to guide an integrated approach. Such an approach would provide a comprehensive solution to any identified security issue rather than the current ad hoc approach. For example, a security architecture would predetermine the security settings for specific groups of assets.

Investing in new technology

Water providers have a forward multi-year program of improvement works to update their corporate and control system environments with more advanced hardware and software to address existing identified security weaknesses, improve functionality and to better align with standards.

Several water providers are considering the future use of low-cost Internet of Things devices to improve the collection of information about localised sections of the water network.

These changes have the potential to improve security as newer equipment inherently has better security features for water providers to use. However, technology will continue to evolve and become more connected reinforcing the need for continuous assessment of vulnerabilities and risks, and the development of an integrated approach to security for control systems.

2.4 Rebalancing security focus

Water providers have focused their attention and resources on the security of their corporate systems. While these systems are important for customer support, communication, and business processes, the interruption of control systems that deliver critical water and sewerage services are equally if not more important.

In the past year, water providers have acknowledged the convergence of these two environments, and two have responded by integrating their business units responsible for these areas to improve service support for both environments.

Penetration testing is an authorised cyberattack on the security of a system to test its strength.

Social engineering involves psychological manipulation of people into performing actions or divulging confidential information.

Phishing is a method of obtaining sensitive information such as usernames and passwords through electronic means—emails and websites—by an attacker masquerading as a trusted entity.

Their risk assessments have resulted in significant investment in securing corporate systems. However, there is opportunity to increase the focus on control systems to address the evolving threat landscape.

Water providers have undertaken some review and penetration testing to confirm the effectiveness of their corporate system security. Water providers have used a range of security activities to either test the strength of their security of corporate systems, or improve their knowledge of these systems, including:

- penetration testing, including social engineering and phishing
- internal audits, reviews and assessments
- physical security reviews
- use of security monitoring tools
- cybersecurity training and awareness
- emergency response training.

However, these activities have not generally extended to their control system environments. We note however that two water providers have conducted limited reviews of their control systems in the past five years.

This focus is inconsistent with the VPDSF, which requires water providers to assess and report their management of information and data security risk, which includes the security practices for control systems.

Extending governance to control systems

Water providers have executive sponsorship for securing both corporate and control systems. However, they have not clearly defined roles and responsibilities for the security of control system assets.

Three water providers have committees or working groups to focus on corporate and control system governance. However, there is limited reporting on control system security at levels 1 to 3, seen in Figure 1B. By not comprehensively assessing their control systems for vulnerabilities and risks at these levels, senior management have not used this information to guide their security decisions.

Building capability

Water providers are recognising the importance of a cybersecurity function within their organisations given the increased threat of internal and external cyberattacks. All water providers have started to build skills specific to control system security, but more needs to be done to enhance expertise in this specialised field.

Non-control system staff undertake key activities that consider the vulnerabilities and risks of the computer systems used in their businesses. These include:

- critical infrastructure assessments
- maintaining and testing emergency management plans and business continuity plans
- establishing a comprehensive security framework including strategy, policy and procedures.

However, staff with relevant expertise in control system security do not sufficiently contribute to these activities, and therefore these activities do not fully incorporate control system issues. There is evidence that this is starting to be addressed at all water providers. Greater involvement of staff with control system knowledge would strengthen the security of these systems and improve emergency management responses.

2.5 Comprehensively assessing security risks

Water providers prioritise the safe and reliable delivery of water and sewerage services, but have not managed the security of the control systems that deliver these services with the same emphasis. There are opportunities to improve the way they secure these systems.

Assessing vulnerabilities and risks

Water providers have not built the security for their control systems based on a detailed understanding of the system assets and their identified security vulnerabilities. This means activities and programs intended to provide security or strengthen existing security, may not address actual system weaknesses. All water providers need to identify their control system assets at the detailed level and the associated vulnerabilities and security risks as the basis for designing and building a suitable security architecture.

Our testing highlighted that staff have knowledge of the control systems they operate, but have a more limited understanding of the detailed security vulnerabilities and risks. None of the water providers have undertaken comprehensive vulnerability assessments of their control systems at the detailed asset and asset zone levels. Where some risks are known, water providers have not thoroughly documented or communicated these to inform existing and new processes.

The ability to complete a detailed security risk assessment requires a comprehensive understanding of control system assets. We found all water providers' asset management records are limited for control systems and do not include detail of the hardware and software in place as the starting point for risk assessment.

Water providers have demonstrated a mature approach to their enterprise risk management with well-established frameworks and processes, and clearly defined risk appetites. They have identified cybersecurity as a strategic risk for both environments and some high-level risks that could impact control systems. However, they are not comprehensively assessing security risks for individual assets and types of assets within the control system environment.

Reliance on compensating controls

Water providers recognise service provision interruption as a critical risk to their business and for this reason control systems have a number of compensating controls—physical redundancy, safety mechanisms and manual operation. However, for some water providers these controls support only short-term business continuity, often through costly manual processes, whereas protecting against a cyberattack can reduce the likelihood of needing to rely on these controls. Reliance on compensating controls is not a replacement for a well-designed security approach.

Physical redundancies and safety mechanisms

Control systems have physical redundancies and safety mechanisms built in because of their importance to service provision. For example, floats and safety shut off valves can detect and prevent an overflow. A cyberattack on control systems might affect these systems in ways not anticipated and so compensating controls may become ineffective. For example, in the power sector, the Stuxnet cyberattack resulted in damage to physical equipment, rendering it inoperable. Operators thought this was a technical fault and continued to replace the damaged equipment while the cyberattack kept running in the background for nearly five years.

Manual operation

If control systems became inoperable due to a successful cyberattack, water providers can manage their assets manually. However, this may require an increase in resources across their geographic area and mean a loss of visibility of operations at remote sites, which may present a challenge if it continued over an extended period. Water providers in Victoria are party to an Australia-wide mutual aid arrangement that provides them with access, on request and if available, to additional resources from other states. However, this may not be sustainable over a long period of time.

Impacts on performance and service delivery

Security interventions such as applying the latest software patches to control systems can, because of the complexity of these systems, have an impact on service performance or reliability. Water providers are cautious about regular patching. They generally take a risk-based approach in applying these patches to minimise potential disruption to systems and services. However, this can put systems at risk of a cyberattack. Our testing found inconsistent application of system patches across most water providers. Water providers must balance the risk of system disruption due to patch application with the risk of system disruption due to cyberattackers exploiting weaknesses caused by out-of-date software.

2.6 Improving response to cybersecurity incidents

Cybersecurity scenario exercises in the water sector

Victoria's all hazards approach to emergency management extends to cybersecurity incidents, driven by requirements under the EM Act and Statement of Obligations. All water providers must conduct an emergency exercise annually. The 2018–19 Water SRP identifies cybersecurity as an area of focus for emergency management response exercises.

MW developed the *Melbourne Metropolitan Water Industry Response Plan* to provide a combined approach to incident response for metropolitan water providers. Under this plan, exercises are conducted every two years and this joint activity can fulfil the requirement for an individual annual emergency exercise for that year.

We observed the October 2018 *Metropolitan Water Industry Response Plan* exercise because of its cyber focus. Four metropolitan water providers participated in the exercise and one attended as an observer. The exercise included website hacking, ransom, water quality issues and loss of control systems for some water providers.

Key learnings from the exercise were shared to support better results for future exercises, or an actual incident. DELWP, DPC, EMV and the Department of Health and Human Services observed, and Victoria Police and representatives of the ACSC attended to observe how the water sector performed and to share insights with participants.

Responding to a control system incident has become part of the emergency management response process. Depending on the severity of an incident, it may be responded to in isolation by control system technicians or scaled up as an organisation-wide, industry-wide or statewide response. In the past year, water providers have included corporate systems staff in these exercises and related emergency training, and are starting to include control system staff, although more control system staff could be included.

The Water Sector Resilience Network has created a collaborative approach to emergency management preparedness within the water sector. Water providers are now engaged and active, both individually and collectively, in preparing for incident response.

Water provider emergency plans and testing

All water providers have an emergency management plan that overarches subordinate business continuity plans that include control systems. They have considered their control systems as an interdependency for key business services in these plans and have adequately assessed the response times and actions needed to recover these. Two water providers are also updating and rationalising their business continuity plans, including refreshing the business impact analysis relevant to control systems.

All water providers have developed disaster recovery plans for their control systems. One has recently begun formally testing their plans and developed a forward testing calendar. The others are informally testing as part of either their upgrade or patching processes, but have not formally documented these tests. This means that they are not capturing learnings from tests to improve their disaster recovery plans.

Appendix A
Audit Act 1994 section 16—submissions and comments

We have consulted with BW, DELWP, EMV—response received from DJCS—MW, VDP and YVW, and we considered their views when reaching our audit conclusions. As required by section 16(3) of the *Audit Act 1994*, we gave a draft copy of this report, or relevant extracts, to those agencies and asked for their submissions and comments. We also provided a copy of the report to DPC.

Responsibility for the accuracy, fairness and balance of those comments rests solely with the agency head.

Responses were received as follows:

BW 34

DELWP 35

DJCS 37

MW 38

YVW 39

RESPONSE provided by the Managing Director, BW

Barwon Water

Our reference:
Your reference: 33605

30 April 2019

Mr Andrew Greaves
Auditor-General
Victorian Auditor-General's Office
Level 31
35 Collins Street
MELBOURNE VIC 3000

Dear Auditor-General, Andrew

RE: Proposed Performance Audit Report Security of Water Infrastructure Control Systems

Thank you for your letter dated 15 April 2019 providing Barwon Water the opportunity to provide comment on the audit report of *Security of Water Infrastructure Control Systems*.

We note the findings of the audit report and welcome the opportunity to identify and implement measures that will further enhance control system security. Barwon Water currently has a number of inflight and planned projects to uplift security of control systems. This program of work has been further informed by the findings of the audit report and will form a comprehensive risk based action plan for monitoring and resolution through our Audit Committee and Board.

Further, we are committed to working with the Department of Environment, Land, Water and Planning in developing an appropriate assurance framework focused on control systems for water infrastructure.

We have appreciated the collaborative approach in undertaking this evaluation.

Yours sincerely

Tracey Slatter
Managing Director

Barwon Region Water Corporation
55 – 67 Ryrie Street, PO Box 659, Geelong, Victoria, 3220
T: 1300 656 007 E: info@barwonwater.vic.gov.au
www.barwonwater.vic.gov.au

Enabling regional prosperity

RESPONSE provided by the Secretary, DELWP

Department of Environment, Land, Water and Planning

PO Box 500, East Melbourne,
Victoria 8002 Australia
delwp.vic.gov.au

Ref: SEC014131

Mr Andrew Greaves
Auditor-General
Victorian Auditor-General's Office
Level 31, 35 Collins Street
MELBOURNE VIC 3000

Dear Auditor-General

PROPOSED PERFORMANCE AUDIT REPORT SECURITY OF WATER INFRASTRUCTURE CONTROL SYSTEM

Thank you for your letter of 15 April 2019 providing the Department of Environment, Land, Water and Planning (DELWP) with the proposed performance audit report on Security of Water Infrastructure Control Systems. The information provided by VAGO through this report will enhance management practices for water infrastructure control systems and strengthen sector governance oversight by DELWP.

Victoria's water corporations and AquaSure for the Victorian Desalination Project (VDP) will remain responsible for the operating technologies for water infrastructure control systems. In responding to the audit's recommendations, DELWP recognises its role as a contract manager for the VDP and in building state-wide water sector resilience. Each water corporation involved in the audit will be providing individual responses to the audit's specific recommendations from an operational perspective. The attached Management Action Plan responds for DELWP as the VDP contract manager.

The audit report highlights the need to improve the cyber-security of control system operating technologies across the water sector. DELWP will continue to work through our water sector resilience networks and with Victoria's Chief Information Security Officer (CISO) to strengthen cyber-security of control systems at a water sector scale by addressing the issues raised in the audit report.

If you would like more information about this matter, please contact Heidi Matkovich, Director, Sector Governance and Support, Water and Catchments, DELWP on 9938 6858 or email Heidi.Matkovich@delwp.vic.gov.au.

Yours sincerely

John Bradley
Secretary

1 / 5 / 19

Encl.

VICTORIA State Government

RESPONSE provided by the Secretary, DELWP–continued

Security of water infrastructure control systems

DELWP's Management Action Plan

Recommendations	Agreed Action	Completion Date
Recommendation #1 DELWP (as the contract manager for the Victorian Desalination Plant) adopt a holistic approach to cybersecurity by integrating security efforts across both the corporate and control system environments (see section 2.3)	**Support** DELWP will confirm AquaSure's proposed actions to adopt a holistic approach to cyber security by harmonising security efforts across VDP's corporate and control system environments and monitor progress.	November 2019 Monitoring - ongoing
Recommendation #2 DELWP (as the contract manager for the Victorian Desalination Plant) clarify roles and responsibilities for control system security governance (see section 2.4)	**Support** DELWP will clarify from AquaSure the roles and responsibilities for control system security governance.	November 2019
Recommendation #3 DELWP (as the contract manager for the Victorian Desalination Plant) identify control system asset security vulnerabilities and risks at the detailed level (see section 2.5)	**Support** DELWP will confirm AquaSure's approach to the identification of control system asset vulnerabilities and risks at the detailed level.	November 2019
Recommendation #4 DELWP (as the contract manager for the Victorian Desalination Plant) design, build and maintain a security architecture proportionate to risk that is based on leading industry security standards for control systems (see section 2.5)	**Support** DELWP will confirm AquaSure's proposed actions to design and build a security architecture proportionate to risk that is based on leading industry security standards for control systems and monitor progress.	November 2019 Monitoring - Ongoing

VICTORIA State Government | Environment, Land, Water and Planning

RESPONSE provided by the Secretary, DJCS

Department of Justice and Community Safety

Secretary

Level 26
121 Exhibition Street
Melbourne Victoria 3000
Telephone: (03) 8684 0501
justice.vic.gov.au
DX: 210077

Our ref: CD/19/287456

Mr Andrew Greaves
Auditor-General
Victorian Auditor-General's Office
Level 31, 35 Collins Street
MELBOURNE VIC 3000

Dear Mr Greaves

Thank you for your letter of 15 April 2019 providing me with the Victorian Auditor-General's Office *Security of Water Infrastructure Control System* proposed draft report and opportunity to formally respond.

The Department of Justice and Community Safety supports the report's findings.

In particular, the department welcomes the Water Sector Resilience Network creating a collaborative approach to emergency management preparedness and notes that water providers are now engaged and active, both individually and collectively, in preparing for incident response.

If you have any questions or would like further information about the department's response please contact Mr Kris Waring, Chief Risk and Audit Officer, on 8684 8280 or by email at Kris.Waring@justice.vic.gov.au.

Yours sincerely

Rebecca Falkingham
Secretary

30/4/19

VICTORIA State Government

RESPONSE provided by the Managing Director, MW

Melbourne Water
Enhancing Life and Liveability

Your ref: File No: 33605

1 May 2019

Andrew Greaves
Auditor-General
Victorian Auditor-General's Office
Level 31/35 Collins St
MELBOURNE VIC 3000

Mr Greaves

Proposed Performance Audit Report *Security of Water Infrastructure Control Systems*

Thank you for the opportunity to provide feedback on the Proposed Performance Report of *Security of Water Infrastructure Control Systems (ICS).*

Melbourne Water recognises the need for, and welcomes the periodic assessment of security requirements for its ICS networks. The threat landscape is constantly changing and the need to secure assets and networks from nefarious threats is no longer restricted to the information technology (IT) environment. An ongoing program of work is underway to identify and address opportunities for improvement and further secure and strengthen the controls supporting both the ICS and IT environments.

Melbourne Water appreciates that this audit has identified opportunities in addition to the remediation program already underway for improvement at both a strategic and tactical level within the ICS environment. As a result, management has developed further actions which will address the key issues and risks identified. Melbourne Water will work together with the Department of Environment, Land, Water and Planning (DELWP) to ensure that the actions taken are aligned with the broader industry-agreed standards, in consultation with the other Victorian water authorities.

The progress of actions in the remediation program will be overseen by the Melbourne Water Board through its Audit, Risk and Finance Committee.

Melbourne Water is committed to a program of continuous improvement to ensure both operational and corporate technology networks within the business are appropriately secured and managed to ensure the best outcome for its customers and stakeholders.

Regards

Michael Wandmaker
Managing Director

Melbourne Water ABN 81 945 386 953
990 La Trobe Street Docklands VIC 3008
PO Box 4342 Melbourne VIC 3001 Australia
TTY 131 722 F +61 3 9679 7099
melbournewater.com.au
Printed on 100% recycled paper

VICTORIA State Government

RESPONSE provided by the Managing Director, YVW

YARRA VALLEY WATER LTD
ABN 93 066 902 501

Lucknow Street
Mitcham Victoria 3132

Private Bag 1
Mitcham Victoria 3132

DX 13204

F (03) 9872 1353

E enquiry@yvw.com.au
yvw.com.au

2 May 2019

Mr Andrew Greaves
Auditor-General
Victorian Auditor General's Office
Level 31/35 Collins Street
MELBOURNE VIC 3000

Dear Mr Greaves,

Proposed Report *Security of Water Infrastructure Control Systems*

Thank you for the opportunity to review and provide feedback on the Proposed Report *Security of Water Infrastructure Control Systems (ICS).*

Yarra Valley Water recognises the need for and welcomes the opportunity to identify and address opportunities for improvement to further secure and strengthen the controls supporting the ICS environment. Our Board and Executive Management Team treat cyber security with the highest of priority and have active oversight of our associated risk profile and on-going programme of cyber security strengthening work. Your Sector report and the specific findings provided to Yarra Valley Water are of great assistance in validation our approach to the security of our ICS.

At Yarra Valley Water we take a risk-based approach to Cyber Security. We have a rolling three-year Cyber Security Strategy refreshed annually, based on an assessment of the risk posed to our organisation. As noted in your findings, we have made a significant investment in the strengthening of our corporate environment in the recent past. This strengthening has included reinforcement of our perimeter security which helps protect our ICS from an external attack.

It is important to note that the security testing undertaken by VAGO for this audit was done from within our secure perimeter with access provided by Yarra Valley Water, and as such this security layer was not tested. With that said, the Board and Executive of Yarra Valley Water appreciate the emerging risk associated with the security of the ICS environment. While at present our ICS are substantially used to monitor rather than control our Operational environment, as the use of technology matures the security of this environment will be of paramount importance.

In recognition of this we are planning to make a significant investment in the security of our ICS environment in the current and future years, in line with our risk based Cyber Security Strategy. As well as investing in cyber security tooling and networking, we are combining our ICS and traditional IT areas into a single Group to ensure a holistic approach to Cyber Security Architectures and practices. Ongoing strengthening of our ICS security will form part of current and future years' plans as our environment and the external landscape evolves.

RESPONSE provided by the Managing Director, YVW–continued

Once again, I would like to take the opportunity to thank you for involving us in this Audit, and in providing both detailed and high level findings that have been valuable in validating our approach to enterprise wide cyber security.

Yours sincerely,

Pat McCafferty
Managing Director
Yarra Valley Water

Auditor-General's reports tabled during 2018–19

Report title	Date tabled
Local Government Insurance Risks (2018–19:1)	July 2018
Managing the Municipal and Industrial Landfill Levy (2018–19:2)	July 2018
School Councils in Government Schools (2018–19:3)	July 2018
Managing Rehabilitation Services in Youth Detention (2018–19:4)	August 2018
Police Management of Property and Exhibits (2018–19:5)	September 2018
Crime Data (2018–19:6)	September 2018
Follow up of Oversight and Accountability of Committees of Management (2018–19:7)	September 2018
Delivering Local Government Services (2018–19:8)	September 2018
Security and Privacy of Surveillance Technologies in Public Places (2018–19:9)	September 2018
Managing the Environmental Impacts of Domestic Wastewater (2018–19:10)	September 2018
Contract Management Capability in DHHS: Service Agreements (2018–19:11)	September 2018
State Purchase Contracts (2018–19:12)	September 2018
Auditor-General's Report on the Annual Financial Report of the State of Victoria: 2017–18 (2018–19:13)	October 2018
Results of 2017–18 Audits: Local Government (2018–19:14)	December 2018
Professional Learning for School Teachers (2018–19:15)	February 2019
Access to Mental Health Services (2018–19:16)	March 2019
Outcomes of Investing in Regional Victoria (2018–19:17)	May 2019
Reporting on Local Government Performance (2018–19:18)	May 2019
Local Government Assets: Asset Management and Compliance (2018–19:19)	May 2019
Compliance with Asset Management Accountability Framework (2018–19:20)	May 2019
Security of Government Buildings (2018–19:21)	May 2019

All reports are available for download in PDF and HTML format on our website
www.audit.vic.gov.au

Victorian Auditor-General's Office
Level 31, 35 Collins Street
Melbourne Vic 3000
AUSTRALIA

Phone +61 3 8601 7000
Email enquiries@audit.vic.gov.au