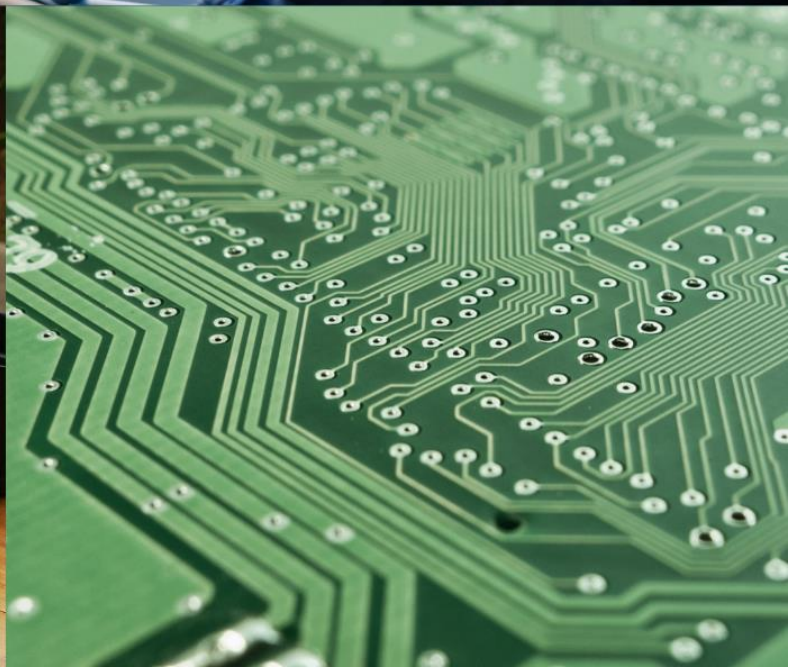
WATER SERVICES
ASSOCIATION OF AUSTRALIA

CYBER SECURITY RESILIENCE PRIMER

FOR DIRECTORS AND EXECUTIVES

FEBRUARY 2023



WATER SERVICES ASSOCIATION OF AUSTRALIA

Contents

1. Introduction

The intent of this guide is to assist Water Utility Directors and Executives in understanding:

- The key questions required to identify critical cyber security risks and ensure business resilience.
- Their regulatory compliance and reporting obligations.
- The risks and the impacts to the organisation if a cyber security incident occurs.
- How the organisation is prepared to respond to a cyber security incident.

2. Cyber security and business risks

Most, if not all, organisations, large or small, especially those with critical infrastructure, are vulnerable to cyber security attacks. The impacts of a successful cyber-attack may include, but are not limited to:

- Theft of customer-sensitive data such as personal addresses, emails, passports, driver's licences, credit card information, etc.
- Disruptions to pump stations, treatment plants and processes such as chemical dozing, opening and closing valves, disabling pumps, etc.
- Loss of control of industrial control systems such as SCADA, resulting in the inability to monitor and control remote operations and other processes.
- Disruption to the entire business processes due to a ransomware cyber-attack.

In addition, cyber security incidents in Water Utilities could impact the reliable delivery of clean and safe water to residents and businesses, negatively impacting the trust and confidence of customers, with potential legal liabilities.

It is important to be aware that cyber security breaches often affect customer information and not just the utility. There is a need for water businesses to focus on the customer during an event, particularly how the business should respond to and support customers.

Once cybercriminals penetrate an organisation's ICT/OT systems, they often demand ransom in exchange for the return of sensitive data or to undo the damage they have done. The Australian Cyber Security Centre (ACSC) has advised organisations who suffer a ransomware attack against paying any ransom because there is no guarantee that lost information will be returned nor that payment will prevent it from being sold or leaked online. In addition, paying a ransom has been shown to increase the likelihood of a repeat attack, and may be a criminal offence.

Paying a ransom could involve committing a criminal offence in the following instances:

- Under the Criminal Code Act - it is an offence to 'deal with' money or property if there is a risk it will become an instrument of crime, and you are reckless or negligent as to the fact the money or property will become an instrument of crime.
- Additionally, the Criminal Code Act makes it illegal to make funds available to a terrorist organisation.
- Charter of the United Nations Act - it is an offence to transfer assets to

sanctioned people and entities or contravene UN sanctions and enforcement laws.

The best way to avoid being a victim of a ransomware attack, or any form of cyber-attacks, is to invest in preventative cyber security measures. These include keeping regular offline backups of business-critical data; patching known security vulnerabilities; regularly testing the effectiveness of current cyber security controls; being aware of and preparing for emerging cyber security threats, and creating a culture of cyber security awareness. No organisation is completely safe from cyber security incidents. However, preventative measures will reduce the risks and are more cost-effective than the comparative costs incurred when attempting to recover from a ransomware incident.

However, despite having in place approaches to avoid ransomware attacks it is almost inevitable that your organisation will at some point be the victim of an attack. The above measures will help detect and neutralise an intrusion, minimising the potential adverse impacts. Probably the most important aspect of recovery from an attack is being able to return all systems to full operation shortly after an attack has been neutralised.

The ACSC has produced guidelines on dealing with ransomware attacks.

- ACSC Ransomware Emergency Response Guide – Recover from a ransomware attack
- ACS Ransomware Emergency Response – One Page Guide
- ACSC Ransomware Prevention Guide

2.1 10 Questions Directors and Executives should ask to understand the business cyber security resilience

To understand the business cyber security resilience, the following are the key questions that should be considered.

No.	Question	No.	Question
1	Do we have a cyber security strategy, and have we assessed how effective it is?	6	How do our suppliers of services, systems, and technologies practice cyber security and provide cyber security assurance for their products and services?
2	Do we have a clear understanding of our cyber security controls and gaps (e.g., ICT, OT systems)? Is there a process to stress test the security of technology and information?	7	How resilient are our cyber security systems (ability to respond to isolated incidents through to a sustained cyber security attack)? Have we tested this using simulations and challenge testing?
3	How often do we review the company's cyber security risks? And why this often? Does this also include constant monitoring of the external operating environment for new and emerging risks?	8	What industry frameworks, standards, best practices and guidelines do we follow and or implement? Are we compliant with relevant legislations requirements (Privacy act, SOCI act, state government legislative requirements)?
4	Do we have a clear picture of what our critical information is?	9	Do we have competent resources to deliver in the event of a potential threat?

5	How do we protect our company's critical information?	10	What is our current cyber security program for the next 12 months?

3. Cyber security Governance

The key to effective cyber security resilience is clarity on roles and responsibilities, strategy, and guidance. Cyber security governance is a set of roles and responsibilities and practices, exercised by those responsible for the organisation's reliance on cyberspace.

The seven governance principles that should be part of every water business's cyber security governance are:

1. **Roles & Responsibilities** – Define clear roles and responsibilities for all.
2. **Cyber security Culture** – Create, promote, and implement a culture of cyber security awareness.
3. **Cyber security/Risk Strategy** – Develop and implement a cyber security strategy, which should be included in the business risk management strategy.
4. **Capability /Resources** – Invest, develop and implement organisational capability to **identify** threats and risks; **detect** cyber security incidents and breaches; **protect** critical information and systems (IT/OT/IoT); **respond** to cyber incidents, including major cyber-attacks; and **recover** from cyber security incidents and attacks.
5. **Regulatory / Legislative Requirements** – meet state and federal legislative compliance and regulatory requirements.
6. **Standards & Best Practices** – adopt relevant standards and guidelines and follow best practices from industry peers.
7. **Threats intelligence** – monitor and stay on top of current and emerging threats to adapt to changing threats and protect the organisation.

The threats of ransomware attacks cannot be discounted, and for water businesses, these threats extend beyond critical information systems to critical infrastructure in OT and IoT systems. Apart from taking proactive actions to harden cyber security controls, water businesses need to develop a response plan to deal with a major cyber security attack. Recovery from a cyber security attack is an essential component of the response plan because it is not a matter of if you will be compromised but when and how quickly your systems can recover.

4. Legislative Requirements

Organisations are obligated by law to be compliant to certain legislative requirements including the Security of Critical Infrastructure Act and the Privacy Act. Water businesses can be liable to government fines for breaching either of these Acts depending on the nature and severity of the security breach along with how it was communicated to government and the public.

3.1 Security of Critical Infrastructure Act

The Security of Critical Infrastructure (SOCI) Act (2018), as amended in 2021 and 2022

applies directly to water businesses with greater than 100,000 property connections or declared by the Minister under Section 51 of the Act, and indirectly to all water businesses (refer to the government SOCI Act page for details). Direct application of the Act in relation to cyber security is embodied in the Rules which accompany the Act. These are currently in development but call up the requirement to develop a cyber security risk management program consistent with or attaining one of several different guideline approaches in including the Australian Signals Directorate Essential 8 or the US NIST guidelines.

The SOCI Act has a requirement for all water businesses to report cyber incidents with the potential to impact the delivery of essential services to the Australian Cyber Security Centre.

3.2 Privacy Act

The Privacy Act 1988 (Privacy Act) was introduced to promote and protect the privacy of individuals and to regulate how Australian Government agencies and organisations with an annual turnover of more than $3 million, and some other organisations, handle personal information.

The Privacy Act includes 13 Australian Privacy Principles (APPs), which are collectively referred to as ‘APP entities’.

The Privacy Act is relevant for retail water businesses holding customer’s personal information.

5. Cyber security Insurance

Cyber security insurance is becoming more difficult to obtain. Key aspects that should require careful consideration are the exclusion clauses in the insurance and the cost to meet the business requirements to obtain insurance, balanced against the risks of self-insurance. In particular, several cyber insurance policies only cover direct consequences of a security breach, not secondary consequences. These direct consequences are often of lower severity and consequence. For example, a breach that affects a control system such as chlorine dosing may have wording that limits damage costs to that of rectifying the dosing unit and connected equipment but not cover the impacts on business reputation, water quality and customers.

Note that when considering the costs of a cyber security attack it is essential to consider the hidden costs associated with recovery. These costs may not be quantifiable in the short term, however, the damage could be long-lasting, including class action taken from customers, reputation damage, a rebuild of the Information Communications Technology (ICT) or Operating Technology (OT), and employee confidence.

6. Cyber security Prioritisation and Mitigation Plans

In developing the cyber security strategy for the business, Water businesses must establish an enterprise cyber security strategy that encapsulates the organisation's current and desired

future cyber security posture, and the business risks it presents. This will help prioritise actions to secure the organisation's ICT and OT environment and systems. Effective implementation of a well-considered cyber security strategy will significantly assist in mitigating business impacts due to cyber security incidents by prioritising important cyber security considerations.

6.1 Cultural change

Embracing cyber security needs to start with everyone in the organisation. It is not just the role of one person or section in the organisation. Activities that could help instil a culture change include:

- Treat cyber security as a critical business imperative
- Create awareness and develop training relevant to the scale and scope of the business
- Implement proactive cyber security measures
- Practice security and safety by design principles for all ICT and OT systems

6.2 Cyber security Assessment

It is advisable for water businesses to review their cyber security practices and postures at least annually. In doing this, the business should evaluate:

- Changes in the threat landscape.
- New vulnerabilities discovered and documented in third-party hardware and software.
- Changes to ICT and OT used by the business.
- How the organisation has grown
- Changes to partnerships and contracts.

A good overall framework to follow is the NIST cyber security framework, or its adapted version by AEMO, the Australian Energy Sector Cyber Security Framework, or AES CSF. In Victoria, the mandated framework is the VPDSF, which incorporates many aspects of the NIST Framework.

Using the NIST, VPDSF or AES CSF guides an organisation in the following aspects of cyber security:

- Cyber security strategy
- Risk management
- Cyber security maturity practices and implementation in various ICT/OT systems, including cloud applications:
  - Business systems
  - Customer systems
  - IT systems
  - Operational Technology systems

The framework also allows an organisation to assess its cyber security maturity level and provide scores for various cyber security domains. This will give valuable insights for an organisation to prioritise its cyber security and mitigation programs.

6.3 Cyber security maturity

Determine how mature an organisation is in terms of its understanding, preparedness, and

ability to identify, protect, detect, respond and recover from cyber security threats. There are several tools that facilitate an understanding of cyber security maturity. For ICT systems, the preferred Australian government framework is the Australian Signals Directorate Essential 8. For OT and non-ICT systems, the US Cyber security Capability Maturity Model (C2M2) provides a helpful starting point.

7. Conclusion

Effective cyber security requires a dedicated cyber security strategy, transparent governance, and an ongoing understanding of how the current threat environment continues to evolve. Effective implementation of a well-considered cyber security strategy will significantly assist in mitigating business impacts due to cyber security incidents by prioritising important cyber security considerations. The business should prepare well for potential incidents including through routine testing of systems and processes. It should look to detection and response, rapid recovery, and transparent engagement with customers.

8. Details of guidelines and standards available to help the sector

Cyber security	Considerations	AU Federal & State Governments Guidelines	International Frameworks, Standards & Guidelines
The critical role of cyber security in business	1. Cyber security & business risks 2. Business impacts due to cyber security incidents 3. Security of Critical Infrastructure 4. Privacy 5. Cyber security Governance 6. Legislature requirements / regulatory compliance	**Federal** 1. ACSC Cyber security Principles 2. Critical Infrastructure Act 3. Privacy Act 4. Essential Eight 5. The Australian Energy Sector Cyber Security Framework & Resources 6. ACSC Advice and Guidance 7. ACSC Ransomware guideline **NSW** 8. NSW Cyber security Policy **Victoria** 9. VPDSF & Standards 10. Structure of the Protective Security Policy Framework	1. Risk Management Framework 2. Security & privacy controls for information systems & organisation 3. NIST Cyber security Framework for Critical Infrastructure 4. NIST Privacy Framework 5. SABSA Enterprise architecture and integrated frameworks 6. COBIT Framework 7. ISO 27001 – the international standard for information security 8. ISO 31000 – the international standard for risk management
The current state of cyber security posture in IT & OT environments	1. Cyber security controls and their effectiveness 2. Cyber security capability 3. Cyber security preparedness 4. Cyber security awareness 5. Identification of vulnerabilities and gaps	**Federal** 1. Information Security Manual - Principles, Guidelines, Terminologies 2. Essential Eight Assessment Process Guide	1. NIST Cyber security Framework 2. Cyber security Capability Maturity Model - C2M2 3. CIS 18 Critical Security Control 4. COBIT Framework 5. Guide to Industrial Control Systems (ICS) Security 6. Guide to Critical Infrastructure Sector - Water and Wastewater systems sector 7. IEC 62443 series 8. Security and Privacy Controls for Information Systems and Organisations 9. Cloud Controls Matrix is a cyber security control framework for cloud computing

Cyber security	Considerations	AU Federal & State Governments Guidelines	International Frameworks, Standards & Guidelines
Regulatory compliance & reporting	1. Critical Infrastructure 2. Privacy Act 3. Essential Eight 4. NSW cyber security framework 5. Victorian legislature requirements	**Federal** 1. Critical Infrastructure Act 2. Privacy Act 3. Essential Eight **NSW** 4. NSW Cyber security Policy **Victoria** 5. VPDSF & Standards	
Industrial IoT Cyber security	IoT Security Principles Practices Guidelines	**Federal** 1. Information Security Manual - Principles, Guidelines, Terminologies 2. IoT Code of Practice - Guidance for Manufacturers 3. ACSC Introduction to securing smart places 4. WSAA IoT Guideline 5. WSAA Digital Reference Framework for the Water Sector 6. IoTAA IoT Security Guideline 7. IoTAA IoT Reference Framework **NSW** 8. NSW Internet of Things Policy Guideline	1. IoT Device Cyber security Capability Core Baseline 2. Foundational Cyber security Activities for IoT Device Manufacturers 3. Considerations for Managing Internet of Things (IoT) Cyber security and Privacy Risks 4. IIC Industrial IoT Security Framework