Jemena Gas Networks (NSW) Ltd

IT Investment Brief – Cybersecurity Program

Non-Recurrent – Maintain and Compliance

Public – 30 June 2024

Glossary

ACSC	Australian Cyber Security Centre
AESCSF	Australian Energy Sector Cyber Security Framework
CABS	Cloud Access Security Broker
capex	Capital Expenditure
CASB	Cloud Access Security Broker
Current regulatory period	The period covering 1 Jul 2020 to 30 Jun 2025
IAM	Identity Access Management
ICT	Information and Communications Technology
IoT	Internet of Things
ISO	International Organization for Standardization
Jemena	Refers to the parent company of Jemena Gas Network
JGN	Jemena Gas Network
Next regulatory period	The period covering 1 July 2025 to 30 June 2030
NIST	National Institute of Science and Technology
NPV	Net Present Value
opex	Operating Expenditure
PAM	Privileged Account Management
RYxx	Regulatory year covering the 12 months to 30 June of year 20xx for years in the Next Regulatory Period. For example, RY25 covers 1 July 2024 to 30 June 2025
SDLC	Systems Development Life Cycle
SOCI	Security of Critical Infrastructure Act
totex	Total Expenditure

Cyber Security Program

Objective	The objective of this initiative is to deploy capabilities in step with technology advancement that provide fit-for-purpose protection and response in line with cybersecurity threats, supporting Jemena Gas Networks (**JGN**) in promoting efficient, safe and reliable service delivery to customers.
Non-recurrent ICT sub-categorisation	☒ Maintaining existing services, functionalities, capability, and/or market benefits ☒ Complying with new/altered regulatory obligations/requirements ☐ New or expanded ICT capability, functions, and services

Background

Cybersecurity is an increasingly prominent threat

Cybersecurity risks continue to challenge companies in Australia and across the critical infrastructure sector. In 2022, cyber incidents reported to the Australian Cyber Security Centre (ACSC)[1] have seen the utility sector move into the top 10 industries based on the volume of reported incidents. The 2022-23 Cyber Threat Report published by the Australian Signals Directorate (ASD) in November 2023[2] highlights that the number of cyber incidents in Australia are maintaining their upward trend. In FY23, approximately 94,000 cyber incidents were reported to the ASD, a 24% increase from the 76,000 reported the previous year and a rate of growth that greatly outstrips the growth in operating businesses. In the same period, 143 cyber security incidents were related to critical infrastructure operational technology and across Australia, significant data breaches resulted in millions of Australians having their information stolen.

Cyber threats are expected to continue to increase, with Gartner[3] predicting that by 2025, 30% of critical infrastructure worldwide will experience a breach that will result in the halting of either operations or mission-critical cyber-physical systems.

Jemena adopts a risk-based approach to cyber threats

Jemena uses the National Institute of Science and Technology (NIST) Cyber Security Framework and the Australian Energy Sector Cyber Security Framework (AESCSF) to assess its cyber-security risk and has an appropriate level of maturity when measured against these frameworks.

In addition to these frameworks, we use threat intelligence from Government and commercial organisations to inform the planning and implementation of appropriate controls and risk-reduction strategies. This approach allows us to deploy controls based on current techniques, tools and procedures used by adversaries today and into the future. Jemena currently uses general cyber security threat intelligence services [redacted] with Operational Technology (OT) specific intelligence provided by [redacted] As products and vendor offerings around security evolve, we may change systems over time.

Jemena's risk-based approach to assessing and managing cyber threats

[redacted]

Jemena applies integrated risk management practices aligned to ISO 31000 international risk management standards to assess and manage cyber and other risks. [redacted] there are several related frameworks, manuals and procedures we adopt to manage risk and cyber threats, including:

- Group Risk Management Manual
- Asset Management Manual
- Crisis and Emergency Management Framework
- Crisis Management Plan
- Emergency Management Plan
- Business Continuity Plan
- Physical Security Framework
- Group Physical Security Manual
- Physical Access Control Procedure

[1] ACSC July 2021 – June 2022 Annual Cyber Threat Report | ACSC (cyber.gov.au)
[2] ASD Cyber threat report 2022- 2023 | ASD (cyber.gov.au)
[3] Gartner predicts 30% of critical infrastructure organisations will experience a security breach by 2025 | Gartner (gartner.com)

- Cyber Security Governance Framework
- Digital Security Incident Response Plan

Cyber risk assessments consider government and industry security threat intelligence and information regarding the unprecedented volume of reported cyber incidents and the gravity of impacts on companies, the community, and individuals.

Recognising the inextricable link between energy security and the management of the electricity and gas systems and markets, the Minister[4] is now proposing the Australian Energy Market Operator deliver additional cyber security functions related to cyber incident response, preparedness, risk and advice.

Jemena considers cyber threats a key contributor to its top operational risks impacting the safe and secure supply of JGN services (refer to Attachment A). As a result, Jemena continually assesses and updates cyber security capability to respond to threat information.

Jemena's cyber security controls

Jemena has a mature and stable cyber security function with ongoing recurrent investment that allows us to manage known risks. Refer to Attachment B - Jemena's Cyber Assurance Framework.

By continually assessing threat intelligence, Jemena has increased its cyber security capability over the past five years, investing in staff and technology to implement key controls as outlined in the table below.

Key Control	Objective / Description
User Awareness	User awareness aims to improve security through mitigating human error, protecting against social engineering and phishing attacks, enabling early threat detection and reporting, ensuring compliance with regulations, and safeguarding the company against malicious attack.
Mail Filtering	Blocks targeted inbound email attacks including credential phishing, business email compromise, supply chain fraud.
Managed Detection and Response	Managed detection and response (**MDR**) is a cyber security service that combines technology and human expertise to perform threat hunting, monitoring, and response of end point devices. MDR enables rapid identification and response to limit the impact of threats.
Network Segmentation	Network segmentation involves partitioning a network into smaller networks with an aim to restrict the level of access to sensitive information, hosts and services.
Vulnerability Management	Vulnerability management is the process of identifying, evaluating, treating, and reporting on security vulnerabilities in systems and the software that runs on them.
Zero Trust Exchange	Isolates network connectivity limiting exposure of services directly to the internet, reducing risks of Distributed denial of service attacks
Geographical Blocking	Automatically restricts access to the corporate system making them accessible from with the Australian geographic region only
Identity Management	Limiting, authorising and managing access to enterprise resources to keep systems and data secure
Security Incident Response	Planned response in preparation to monitor, contain, eradicated bad actors or malware resulting from a cyberattack
System Backup	Backups enable recovery of systems and encrypted or lost data
Disaster Recovery	Plans, processes and capability to restore Digital systems and data after an event that disrupts Digital operations, such as a natural disaster, a cyberattack, or a hardware failure.

Customer Importance	ICT is a primary enabler of JGN's ability to operate a safe, reliable, and efficient distribution network. Cyber security risk is the most probable harm that could cause the widest possible impact on the safe and reliable delivery of gas to our customers.

[4] Rule Change request, Australian Energy Market Operator – Cyber Security Role, March 2024 | Australian Government DCCEEW (AEMC.gov.au)

[redacted]

cyber-attack on Jemena's ICT systems, whether targeted, opportunistic, or indirect, will have a significant customer impact if not managed effectively:

- Smart network devices, if taken control of remotely by malicious attackers, could impact the supply of gas, cause damage to equipment and expose the public to risks of fire and explosion.
- Spoofing of work orders and instructions to field staff could result in JGN workers unknowingly causing impact services on parts of the network that only support the manual operation.
- If computer systems relied upon by field and office staff are disabled, JGN will lose the ability to operate its business, which may impact the integrity of customer billing, result in longer outages and increase operating costs.
- The theft of sensitive customer data could also adversely affect customers and reduce trust in JGN.

JGN's priority is to maintain the supply of gas, operate a safe and reliable energy network and protect customer data and information. To meet customer expectations for safe and reliable gas supply Jemena must continue to invest in capability to identify, protect, detect, respond and recover from cyberattacks.

Key Considerations

Continued investment in Cybersecurity is required to keep pace with cyber threats

Advancements in the technology areas of data analytics, cloud adoption and smart integrated networks are quickly transforming how assets and ICT processes are applied and operated.

Digitisation and cloud adoption are forcing companies to shift away from traditional ICT perpetual licensing and owner-operator models from the past to technology services hosted externally and maintained by external 3rd parties, driven through operating efficiencies and reduced total cost of ownership benefits.

[redacted]

Technology advances benefit company efficiency and generates opportunities for cybercriminals to apply new tactics, tools, and processes. Jemena must continue to deploy cybersecurity capabilities with technological advancements that provide fit-for-purpose protection and response in line with current and emerging cyber security threats.

[redacted]

To meet customer expectations for safe and reliable gas supply [redacted] Jemena must continue to invest in systems to identify, protect, detect, respond and recover from cyberattacks.

As trends in cyber security threats grow, so do government laws, rules and regulations aimed at protecting consumers subjected to those risks. This parallel trend means that Jemena needs to meet the actual threat as well as the expectations placed on it by governments in the 2025-30 period.

With our ongoing program to maintain existing cyber security capabilities, this investment brief proposes a threat-based and risk-based approach to uplifting JGN's cyber security capabilities to minimise and mitigate increasing cyber security threats.

Options

JGN has considered two alternatives to deliver the capability articulated above:

(1) Do nothing - Maintain existing cyber security controls

(2) Implementation of additional fit-for-purpose cyber security controls to continue to manage cyber threats.

Option 1: Do nothing

Description

Maintain our existing cyber security controls (refer to the Background section) which are covered under operating expenditure. No additional capability will be implemented to mitigate against increasing cyber threats as assessed as part of our CI Risk Management Plan.

Benefits

Expenditure levels are maintained, with no short-term additional operational expenditure outlay.

Risks

Taking a do nothing approach to keep up with the security of the gas network materially increases the likelihood of a successful cyberattack that impacts the safe supply of gas to our customers. Over time the probability of success increases as the gap widens between control effectiveness and threats as controls become out of step with criminal tactics. Doing nothing has the safe effect of reducing control effectiveness over time.

Jemena considers the risk rating of maintaining the status quo to be high due to increased vulnerabilities. [redacted]

Summary

This option is not recommended. This option will expose JGN to an increasing likelihood of a successful cyberattack with networks and customer implications, and JGN considers that it does not reflect good industry practice.

Option 2: Implement fit-for-purpose cyber security controls

Description

In addition to maintaining our existing cyber security controls, the cyber security program comprises several additional security capabilities, all of which will contribute to the continued security of the JGN network, systems and data. These are described further below:

- [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
- [redacted]

[redacted]

- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Costs

$2023	RY26	RY27	RY28	RY29	RY30
Total Capex					
Non-recurrent Opex	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Recurrent-step Opex		[redacted]	[redacted]	[redacted]	[redacted]
Total Opex	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Totex	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

This is an Enterprise-wide initiative; Costs have been allocated in accordance with Jemena Group Cost Allocation Methodology.

The forecast non-recurrent opex is [redacted]

Summary

Delivery of cyber security capability will embed cyber controls in step with technology advancement providing fit-for-purpose protection and response in line with cybersecurity threats, supporting JGN in the safe and reliable operation of the Jemena gas network. This option is recommended as we consider it reflects good industry practice given the benefits and risks outlined above.

Options Summary

The table below summarises the quantitative and qualitative differences between the analysed options.

Refer to Attachment A for Risk assessment.

	Capex ($2023)	Project opex ($2023)	Ongoing opex ($2023)	NPV	Residual Risk
Option 1	Not applicable	Not applicable	Not applicable	Not applicable	High
Option 2	$0	[redacted]	[redacted]	[redacted]	Significant (refer attachment A)

What We Are Recommending

Jemena recommends option 2. This will support cybersecurity requirements [redacted], and JGN considers that it best reflects good industry practice.

This option is recommended as we consider it reflects good industry practice given the benefits and risks outlined above. Furthermore, it provides the lowest sustainable cost.

Dependencies on other Investment Briefs

Not applicable.

Relationship to ICT Capital Forecast

The supporting modelling for this investment brief is contained in the following investment framework model: **JGN - RIN - 4.3.5 - ICT Investment Brief – Cybersecurity Program – Costs and Benefits Analysis Model**

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]