Australian Academy of Technological Sciences & Engineering

REPORT SUMMARY

FORTINET



Strengthening the resilience and integrity of Australia's critical operational systems

Securing the systems of modern Australian life.

EXECUTIVE SUMMARY

Our daily life depends on Australia's critical operational systems and infrastructure: the electricity and gas networks, the water and wastewater plants, the hospitals, the ports and freight routes, the payment systems, and the phone and data networks. They are invisible, until they stop working. When one of our operational systems stops, the services that depend on it stop with it.

This report examines the cyber security of these interconnected systems. It asks how the systems depend on one another, how a disruption in one spreads to others, where responsibility for that risk sits, and what it takes to keep the systems running.

The connection between information technology (IT) and operational technology (OT), once kept separate, now provides a route for attack. Vulnerabilities are frequently exploited within weeks of disclosure, and AI is shortening that interval further.

Australia's existing regulation and action environment is primarily formed by the Security of Critical Infrastructure Act 2018 (the SOCI Act), the Critical Infrastructure Resilience Strategy and the Trusted Information Sharing Network. Together, these can be built up to better strengthen the resilience and integrity of critical national infrastructure.

Key issues and recommendations to address them

Addressing the key cybersecurity issues facing the critical infrastructure sector requires shared information, practice and capability across operators, which regulation on its own does not create.

Two conditions run through all six issues:

Convergence, where equipment that was once secured by isolation is now connected to corporate networks and through them to the internet

Interdependency, where a service failure also disrupts the services that depend on it, so the consequence of a failure is set by what relies on the system, whatever the size of its operator.



ISSUE 1

Dependencies are often unknown.

Cascading failure, where the loss of one service disrupts the services in other sectors that depend on it, is one of the most consequential risks to Australia's critical infrastructure.

RECOMMENDATION 1

Create a national assessment of Australia's critical infrastructure dependencies, share it regularly with the governments and operators who need it, and establish clear responsibility for its ongoing delivery.

ISSUE 2

Operators are responsible for equipment and services they did not build.

Most equipment that runs physical processes was engineered in an era when it was not able to communicate externally. Those design decisions from the time of construction now create risks that need to be managed by modern operators.

RECOMMENDATION 2

Make protection between systems the expectation, and support operators and suppliers to share responsibility for the security of what is sold and supported.

ISSUE 3

Capability across operations, IT and governance is scarce and uneven.

Resilience in OT environments requires people who understand industrial operations, IT, the associated governance expectations, and now AI as well. Risks that cross the boundary between an operations team and an IT team, or between an operator and its regulator, can fall between them.

RECOMMENDATION 3

Build capability where operations, IT and governance meet, and support the operators least able to build it alone.

ISSUE 4

Information can become stuck when it is needed most.

Incident information serves to notify government, warn other operators with enough detail to act on, and tell the public what is happening and what to do. Arrangements for public disclosure and information sharing among operators are known issues.

RECOMMENDATION 4

Give operators permission and the means to share information and experience on cyber incidents in critical infrastructure, and build a shared way to assess AI and emerging technology risks.

ISSUE 5

We do not measure whether resilience is improving.

Australia can describe its critical infrastructure regime in detail, but no Australian source measures whether outages have become shorter, recovery faster or cascading failures rarer since reporting obligations commenced.

RECOMMENDATION 5

Measure resilience against service outcomes, and bring the testing that already happens into one national view.

ISSUE 6

Digital and AI infrastructure is not yet recognised as critical.

Every sector this report covers now depends on digital and AI infrastructure. Communications, energy, health, transport and water run on data centres, cloud services and AI compute. That dependence is concentrated, but not reflected as such in practice.

RECOMMENDATION 6

Recognise digital and AI infrastructure as critical, in regulation and in national planning and investment.

Filling a data gap

Several of these recommendations depend on evidence Australia does not yet collect, and the gaps are a research agenda in themselves:

- a consolidated national assessment of dependency between critical services
- Australian data for cascading-risk modelling, which is validated on synthetic or overseas data at present
- a representative account of the OT security workforce
- evidence on the condition of the equipment that workforce maintains
- an agreed set of resilience outcome measures
- the extent of dependence on digital and AI infrastructure
- an assessment of whether the frameworks Australia applies have made services more resilient.

Next steps for Australia

Taken together, the recommendations provided here would produce a national picture of dependency, a clear owner for the risks between organisations, and the evidence to tell whether resilience is improving.

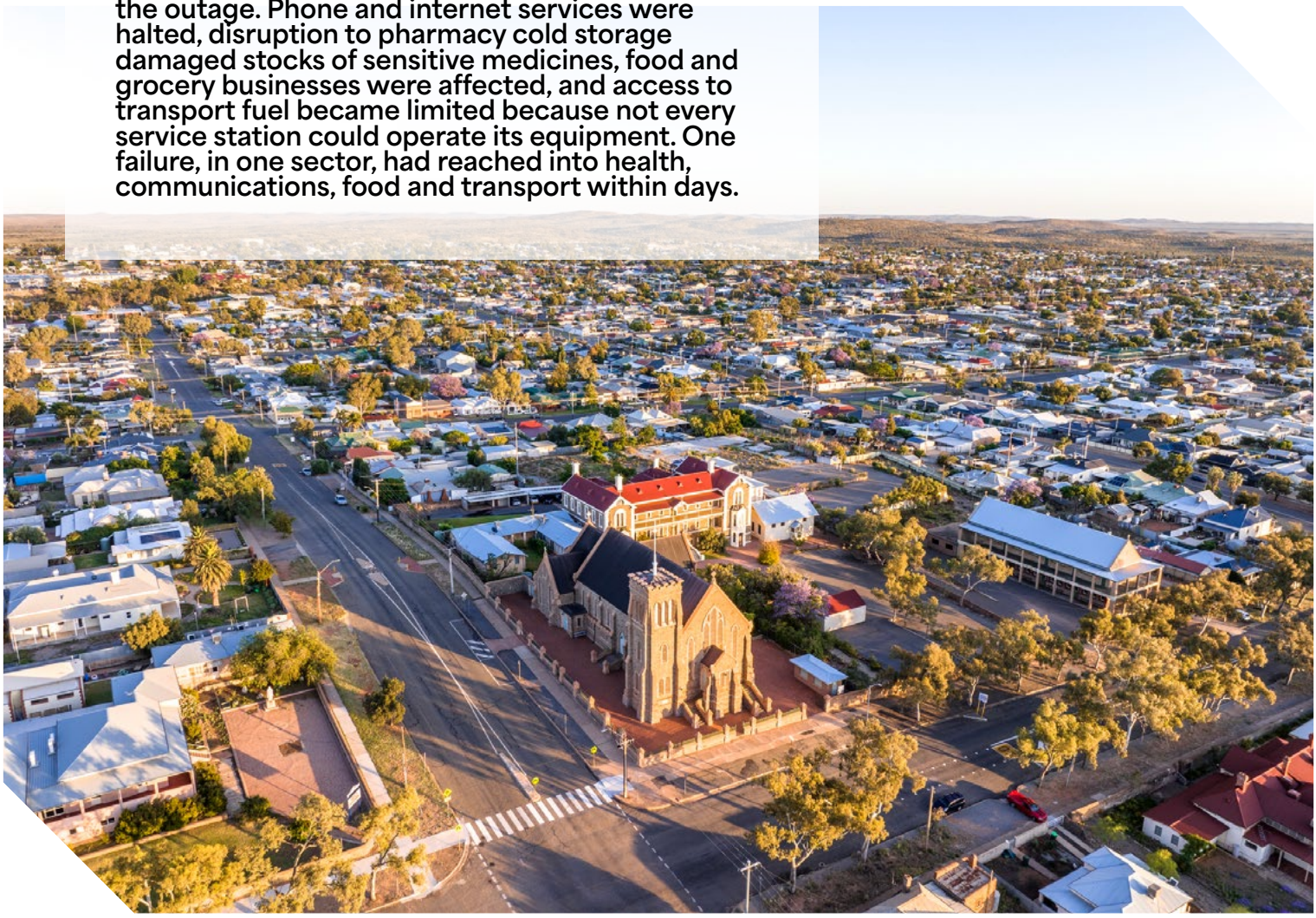
These arrangements can strengthen the resilience of the critical operational systems on which Australian communities depend.

Full report QR

CASE STUDY

Cascading infrastructure failures in Broken Hill, October 2024

Severe weather damaged the transmission lines supplying Broken Hill with power, and, less than a week later, the generator brought in for backup power overheated and tripped, extending the outage. Phone and internet services were halted, disruption to pharmacy cold storage damaged stocks of sensitive medicines, food and grocery businesses were affected, and access to transport fuel became limited because not every service station could operate its equipment. One failure, in one sector, had reached into health, communications, food and transport within days.



ATSE Australian Academy of Technological Sciences & Engineering

The Australian Academy of Technological Sciences and Engineering (ATSE) is a Learned Academy of independent, non-political experts helping Australians understand and use technology to solve complex problems. Bringing together Australia's leading thinkers in applied science, technology and engineering, ATSE provides impartial, practical and evidence-based advice on achieving sustainable solutions and advancing prosperity.

FORTINET

Fortinet is a driving force in cybersecurity, delivering integrated protection for digital and operational systems that people, economies and communities rely on. The Fortinet Security Fabric combines secure networking, Unified SASE and security operations in an AI-powered platform, improving visibility and coordinating protection, detection and response across IT, OT and cloud. Trusted by over one million customers, Fortinet strengthens resilience through the industry's largest integrated cybersecurity portfolio, threat intelligence and collaboration with government, industry and academia.