FUTURE GOVERNMENT INSTITUTE
Powered by Public Sector Network

STRENGTHENING THE SHIELD: ADVANCING WHOLE-OF-GOVERNMENT CYBER RESILIENCE

EXECUTIVE SUMMARY | VOL.24 | FEDERAL | QUT CANBERRA EXECUTIVE EDUCATION CENTRE

IN BRIEF

The Future Government Institute Research Council, in partnership with QUT, convened a Chatham House roundtable exploring how cyber resilience can be elevated as a whole-of-government priority to ensure public trust and service continuity. The session brought together senior executives from federal departments, cybersecurity experts, and industry partners to assess maturity levels, workforce challenges, foundational gaps, and collaboration opportunities within the public sector cyber landscape.

A key insight was the uneven maturity across agencies, with most positioned at intermediate levels of cyber resilience. While some benefit from incident-driven investment, others lag due to systemic issues like legacy systems and siloed risk governance. Skills shortages, cross-agency collaboration failures, and fragmented governance models emerged as core obstacles. The group called for stronger workforce development via APS-wide initiatives, enhanced cross-sector intelligence sharing, and executive education in cyber literacy.

The session also revealed deep concerns about sovereign capability in cybersecurity, drawing parallels to past challenges in cloud adoption. Participants emphasised the need for federated approaches to system and data modernisation, modular workforce planning, and a more assertive stance on integrating secure-by-design practices. These findings provide a roadmap for aligning cyber strategies with whole-of-government service transformation.

By **Patrick Joy** | Head of Research & Analysis | **Public Sector Network**

KEY THEMES AND INSIGHTS

CYBER RESILIENCE IS A MATURITY CONTINUUM, NOT A FIXED STATUS

Participants placed their agencies on a spectrum from basic compliance to strategic integration of cybersecurity. Most agencies self-assessed at an "intermediate" stage, marked by policy implementation, known gaps, and variable interoperability. A select few described advanced practices—embedding cyber into governance and cultivating trusted relationships with intelligence agencies—but these were exceptions.

Notably, some cited past cyber incidents as catalysts for executive focus and investment. One department reflected that a public breach in 2019 transformed cybersecurity from an IT concern into an executive priority, bringing funding, resourcing, and sustained governance attention. However, others warned against crisis-driven progress and emphasised proactive governance.

LEADERSHIP ENGAGEMENT IS ESSENTIAL BUT INCONSISTENT

Several contributors noted that despite increasing senior awareness, many SES and governance boards still treat cyber risk perfunctorily. Cyber is often placed in risk registers without meaningful action. ASD and ACSC outreach was acknowledged as improving, but many felt their engagement remains skewed toward national security agencies, excluding much of the APS.

The lack of common frameworks to translate technical risk into business context was cited as a critical gap. Participants stressed the need for better executive cyber literacy and structured pathways for communicating cyber risk in plain, strategic terms.

LEGACY SYSTEMS AND DATA SILOS UNDERMINE CYBER READINESS

Many agencies operate critical services on decades-old systems, some built on unsupported platforms. These inhibit not only agility but also create fragmented data environments that complicate cyber governance. One agency highlighted maintaining separate systems for individuals performing multiple roles (e.g. marriage celebrant and family mediator) due to siloed data structures.

The consensus was that system modernisation must go hand-in-hand with information governance. Without clarity on data location, ownership, and provenance, even basic cyber hygiene becomes impossible. Attempts at inter-agency integration have largely failed due to incompatible systems, cultural resistance, and lack of common processes.

COLLABORATION EXISTS, BUT AT THE MARGINS

While some progress has been made—such as PDMS creating a common document management platform—examples of genuine system or capability sharing remain rare. Participants highlighted fragmented software procurement, inconsistent toolsets, and the absence of coordinated incident response mechanisms across agencies.
The use of threat intelligence sharing among Five Eyes allies was cited as a potential model for cross-agency collaboration. Participants stressed the need for scalable models to share vulnerability intelligence, risk assessments, and even cyber talent.

CHALLENGES AND BARRIERS

STRUCTURAL AND CULTURAL BARRIERS

A recurring theme was the siloed nature of APS departments and the absence of incentives for collaboration. Agencies were reluctant to share data due to accountability fears—concerned that poor-quality data or decisions based on it might invite scrutiny or blame. A risk-averse culture further inhibits openness and experimentation.

WORKFORCE GAPS AND PIPELINE CONSTRAINTS

Participants raised alarms about the acute shortage of cyber skills in the APS. Many cyber roles draw from the same limited ICT graduate pool, 85% of whom are international students and therefore not eligible for many government roles. Agencies struggle to retain cyber talent due to uncompetitive pay, lack of career pathways, and HR constraints on mobility.

LEGACY TECHNOLOGIES AND POLICY INERTIA

Legacy platforms not only constrain security posture but repel new talent. New entrants often seek modern, cloud-native environments, not COBOL and mainframes. Yet, transitioning away from legacy is hindered by policy constraints, lack of funding, and competing priorities.

SOVEREIGN CAPABILITY AND SECURE DEVELOPMENT

Concerns were raised that Australia is again falling behind on sovereign technology capability, as happened with cloud and potentially now AI. The roundtable recommended strategic investment in local solutions and the development of secure-by-design frameworks that balance innovation with control.

FUTURE FOCUS AREAS

SES CYBER LITERACY AND LEADERSHIP ENABLEMENT

A call was made to institutionalise executive-level cyber training, potentially as a modular offering within APS Academy leadership programs. This would build awareness and equip decision-makers to assess risk, understand threat landscapes, and support risk mitigation.

WHOLE-OF-APS CYBER WORKFORCE PLANNING

Participants strongly endorsed the Data, Digital and Cyber Workforce Plan launched in March. There was consensus that successful implementation requires breaking out of siloed hiring practices, expanding beyond graduate pipelines, and fostering career pathways for reskilled or transitioning professionals. Micro-credentialling and modular upskilling were suggested as scalable options.

EXPERIMENTATION AT SCALE

Innovation labs and structured hackathons were cited as powerful enablers of internal transformation. Participants called for the establishment of shared experimentation environments—"safe spaces" with vendor partnerships and low-risk funding models—to enable early-stage prototyping of AI and automation tools across agencies.

COMMON CAPABILITY PLATFORMS AND INVENTORY MAPPING

Participants proposed broader mapping of commonly used toolsets (e.g. Microsoft 365, Ivanti MobileIron) to enable coordinated incident response and investment. A government-wide inventory of critical platforms and vulnerabilities would support proactive, collective mitigation.

INNOVATIVE IDEAS AND CASE STUDIES

1. EMBEDDED INDUSTRY COLLABORATION AND TALENT EXCHANGE

Some agencies noted successful partnerships where ASD embedded staff into agency teams for specific cyber uplift initiatives. This model of embedded collaboration—with knowledge transfer as a core objective—was seen as a scalable template for improving sector-wide capability.

One department shared a novel arrangement: a cyber contractor who left to join ASD was later re-deployed back into the agency via the SPICE program. This informal talent exchange enabled continuity of expertise and demonstrated how inter-agency cooperation could work in practice.

2. CYBER HYGIENE THROUGH PLATFORM ENGINEERING

Industry participants presented a case for platform-based DevSecOps and secure software supply chains. One vendor described how a proactive alert to a client about an active exploit allowed for rapid patching and system recovery. This "fix-once, apply-many" model enables higher hygiene levels at lower cost.

Another case outlined how DevOps automation was extended to mainframes—allowing legacy systems to integrate with modern CI/CD pipelines. This reduced the siloing of skills and helped attract a new generation of technologists to support secure legacy transformation.

3. GOVERNANCE MODELS FOR RISK CONTEXTUALISATION

Several participants emphasised that cyber governance must shift from compliance reporting to contextual risk understanding. Agencies that successfully bridged technical and strategic domains were able to communicate cyber risk through frameworks like "crown jewels" analysis and defence-in-depth models.

STRATEGIC OUTCOMES AND RECOMMENDATIONS

IMMEDIATE ACTIONS

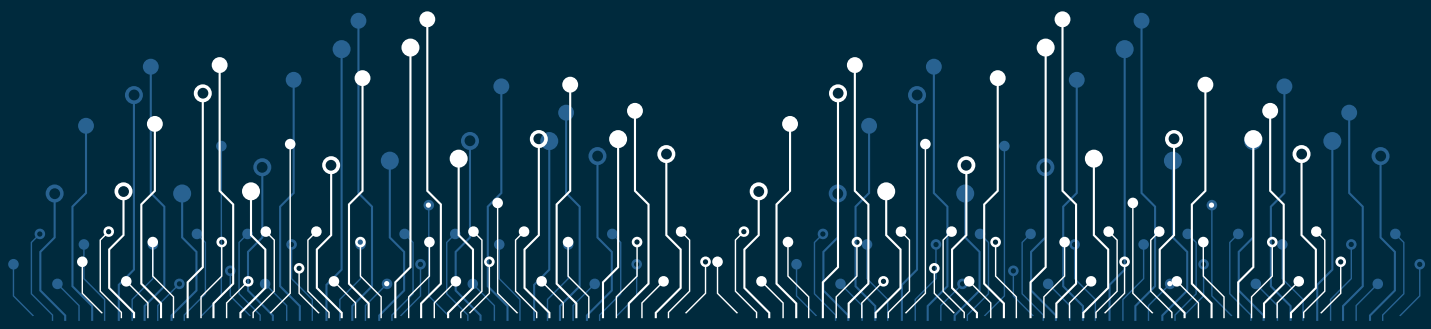
- Launch modular cyber literacy programs for SES through institutions like APS Academy, Public Sector Network Academy, and the Future Government Institute.
- Establish an APS-wide register of core platforms (e.g. Microsoft 365, Ivanti) and vulnerability profiles.
- Incentivise more agencies to join ASD's scenario response and cyber exercise programs.

MEDIUM-TERM GOALS

- Formalise inter-agency talent exchanges in cyber, mirroring successful embedded support models.
- Create a cross-agency micro-credential framework in partnership with academia and industry.
- Standardise procurement and risk assessment for common software and SaaS platforms to minimise duplication and enhance transparency.

LONG-TERM VISION

- Modernise legacy systems with secure interfaces and DevSecOps integration, prioritising high-impact business systems.
- Develop sovereign cybersecurity capability and strategy, with a focus on talent retention, threat intelligence, and secure-by-design infrastructure.
- Embed cyber resilience into whole-of-government transformation planning, aligned to digital trust and public confidence measures.



ABOUT THE FUTURE GOVERNMENT INSTITUTE (FGI) RESEARCH COUNCIL

We've been able to engineer a new program antithetical to the classical red tape, administration, and risk-aversion that impedes innovation.

Public Sector Network has recently launched The Future Government Institute (FGI), a global hub for forward-thinking public sector leaders, innovators, and practitioners dedicated to shaping the next era of governance.

Our mission is to empower government professionals with the tools, insights, and networks needed to drive meaningful transformation - https://publicsectornetwork.com/future-government-institute/

Leveraging our extensive connections, we are uniting the sharpest minds from government, academia, and industry via monthly research-driven roundtables, hosted at esteemed national centres of research, courtesy of university partners across Australia and New Zealand.

ABOUT PUBLIC SECTOR NETWORK

Public Sector Network is a research company that represents public sector professionals across Australia, Canada, New Zealand, and the USA. It develops roundtables, seminars, and conferences to suit current areas of interest to government agencies and their suppliers.

PSN's growing community spans across federal, state, and local government departments, healthcare, and education, allowing members to share information, access the latest in government innovation, and engage with other like-minded individuals on a secure and closed-door network.

AUSTRALIA / NEW ZEALAND
P +61 2 9057 9070
E INFO@PUBLICSECTORNETWORK.COM.AU

USA
P +1 (647) 969 4509
E HELLO@PUBLICSECTORNETWORK.COM

CANADA
P +1 (647) 459 8904
E CONTACT@PUBLICSECTORNETWORK.CO

Public Sector Network (Australia) Pty Ltd
ABN - 46 617 870 872 20-40
Meagher Street, Chippendale, Sydney NSW 2008, Australia