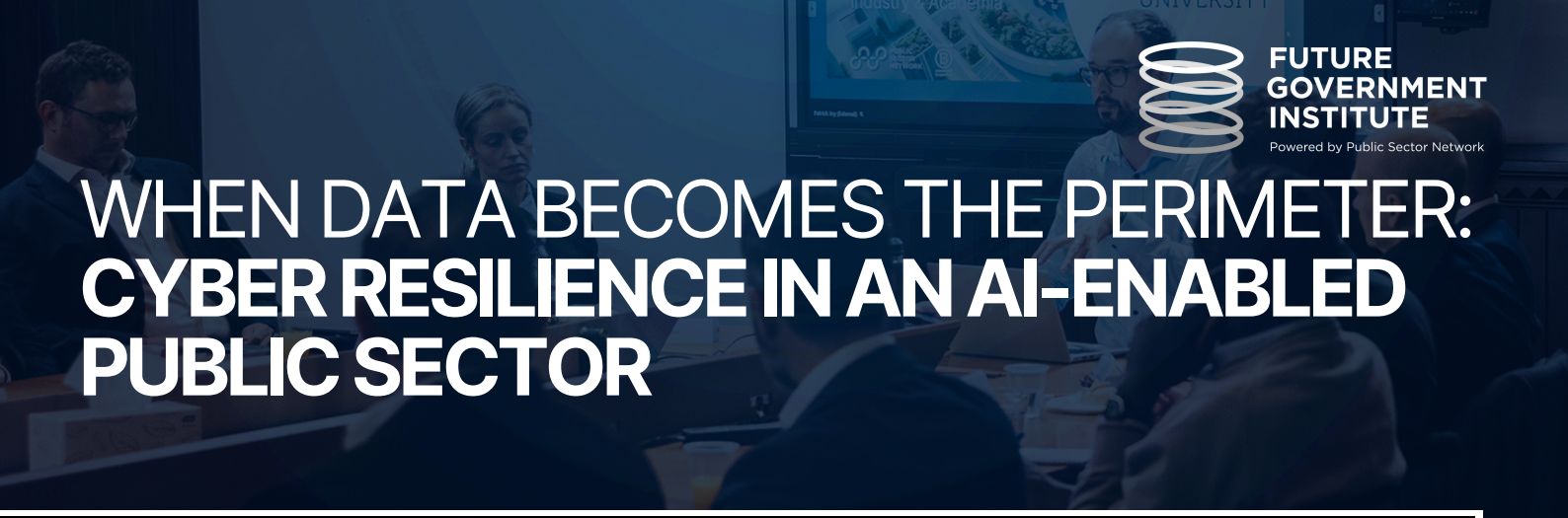


FUTURE GOVERNMENT INSTITUTE
Powered by Public Sector Network

WHEN DATA BECOMES THE PERIMETER: CYBER RESILIENCE IN AN AI-ENABLED PUBLIC SECTOR

EXECUTIVE SUMMARY | VOL.34 | NEW SOUTH WALES

UTS UNIVERSITY OF TECHNOLOGY SYDNEY

IN BRIEF

The Research Council convened a roundtable at the University of Technology Sydney to examine cyber resilience as a foundational capability for government, rather than a narrow technical function. While artificial intelligence was not the primary focus, participants consistently highlighted its accelerating impact on cyber threat vectors, workforce behaviours, and data governance practices. A central insight was that cyber maturity is not a fixed end state. Instead, agencies described a continuous cycle of readiness, adaptation, and resilience, shaped by evolving technologies, regulatory obligations, and threat actors.

Discussions revealed wide variation in organisational maturity, with most participants positioning their agencies at an intermediate stage. While many have adopted baseline controls such as Essential Eight, identity management, and incident response simulations, deeper challenges persist around unstructured data, legacy systems, and third-party dependencies. Participants emphasised that up to 80 to 90 per cent of government data remains unstructured, significantly increasing exposure during breaches and complicating compliance with retention, deletion, and right-to-forget obligations.

A recurring theme was the distinction between security and resilience. High-profile incidents were cited to illustrate that systems can remain operational while data is compromised, or conversely fail catastrophically without a security breach. This reinforced the need for "resilience by design", particularly for services of government importance and citizen-facing systems.

The roundtable underscored that sustainable cyber resilience depends on leadership engagement, technology-enabled controls that reduce reliance on human perfection, and cross-sector collaboration. Facilities such as secure research environments, shared threat intelligence networks, and workforce capability programs were identified as practical enablers to lift system-wide resilience across government and its partners.

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

KEY THEMES AND INSIGHTS

CYBER MATURITY IS A MOVING TARGET, NOT A DESTINATION

Participants consistently rejected the notion of a "fully mature" cyber posture. Even organisations with advanced controls described cyber as an ongoing arms race, shaped by rapidly changing technologies, threat tactics, and regulatory expectations. Several participants noted that maturity frameworks often lag reality, creating a false sense of assurance once compliance thresholds are met.

This was particularly evident in discussions of Essential Eight implementation. While many agencies comply at baseline or risk-adjusted levels, participants stressed that compliance alone does not equate to resilience. As one contributor observed, the threat landscape evolves faster than policy cycles, meaning yesterday's controls can quickly become today's vulnerabilities. This reinforces the need for continuous monitoring, adaptive governance, and investment models that support ongoing uplift rather than one-off remediation programs.

DATA IS THE NEW ATTACK SURFACE

Data governance emerged as one of the most critical and unresolved challenges. Agencies described holding decades of legacy data, including records dating back to the 1970s, often without clear retention justification or ownership. Participants highlighted that organisations cannot protect what they do not understand, and many lack comprehensive visibility of where sensitive data resides, who can access it, and how it flows across systems.

Unstructured data was repeatedly identified as the highest-risk category. Estimates suggested that 80 to 90 per cent of organisational data sits in emails, documents, and collaboration platforms, outside traditional database controls. This significantly increases exposure during incidents and complicates incident response, forensic analysis, and Freedom of Information requests. Several contributors argued that improving data classification, labelling, and reduction is a prerequisite for safe AI adoption, as AI systems will inevitably surface data risks that already exist.

SECURITY AND RESILIENCE ARE NOT THE SAME THING

A key conceptual distinction emerged between security and resilience, which participants argued are often conflated in policy and operational discussions. Examples were used to illustrate that a system can be secure but not resilient, or resilient but not secure. In one case, a global technology outage demonstrated how a non-malicious failure could halt essential services despite no breach occurring. In contrast, major data breaches showed that services can remain operational while public trust is severely damaged.

This distinction has significant implications for government. Participants stressed that citizen-facing services must be designed to continue operating under failure conditions, whether caused by cyber attacks, supply chain disruptions, or system faults. Resilience by design was positioned as an essential principle for critical infrastructure, health, education, and social services, where service continuity often matters as much as data confidentiality.

HUMANS ARE NOT THE WEAKEST LINK, BUT THEY CANNOT BE THE CONTROL

While social engineering remains the dominant attack vector, participants challenged the framing of users as the weakest link. Instead, they argued that systems should assume human error and be designed to prevent catastrophic consequences when mistakes occur. AI-enabled phishing, deepfake voice calls, and context-aware impersonation were cited as making traditional awareness cues such as spelling errors obsolete.

Effective approaches described included simulated phishing exercises, contextual training that teaches staff to question plausibility rather than appearance, and technology controls that nudge or block risky behaviour. Participants emphasised that controls must be easy and unobtrusive. If security processes slow people down or obstruct their work, users will bypass them, often in ways that increase risk.

CHALLENGES AND BARRIERS

LEGACY SYSTEMS AND DATA ACCUMULATION

Legacy platforms were repeatedly cited as a structural barrier to resilience. Many agencies operate mainframes and bespoke systems that are deeply embedded in business processes, making decommissioning costly and risky. These systems often hold vast quantities of historical data, increasing exposure while delivering limited operational value. Participants noted that fear of deleting data, driven by unclear retention rules and regulatory anxiety, leads to chronic over-retention and inflated risk profiles.

FRAGMENTED IDENTITY AND ACCESS MANAGEMENT

Federated identity models, particularly across education, health, and community services, were identified as a persistent challenge. Agencies described managing multiple identity stores for staff, students, partners, and citizens, often with inconsistent authentication standards. This fragmentation increases the attack surface and complicates incident response. While centralised identity initiatives are underway, participants acknowledged that edge cases such as minors, vulnerable populations, and low-access users complicate implementation.

WORKFORCE CAPACITY AND COGNITIVE LOAD

Participants highlighted the unsustainable pressure placed on cyber teams, who are expected to manage technical controls, regulatory compliance, incident response, and organisational change simultaneously. Many teams lack the capacity to think proactively about emerging threats such as quantum decryption, agentic AI, or next-generation networks, because they are consumed by day-to-day firefighting. This reactive posture increases long-term risk.

FUTURE FOCUS AREAS

RESILIENCE BY DESIGN FOR SERVICES OF GOVERNMENT IMPORTANCE

Future work should focus on defining and operationalising resilience by design for critical and citizen-facing services. This includes dependency mapping across third-party providers, open-source components, and shared platforms, as well as stress-testing services against non-malicious failures and cascading outages. Capability development in this area would support compliance with critical infrastructure obligations while improving service continuity.

DATA REDUCTION, CLASSIFICATION, AND DELETION

Participants identified a clear need for practical guidance and shared capability around data reduction. Future Research Council activity could explore scalable approaches to data classification, context-aware retention, and defensible deletion, particularly for unstructured data. This would directly reduce cyber exposure and enable safer AI deployment.

HUMAN-CENTRED CYBER CAPABILITY

There is an opportunity to reframe cyber education around individuals, not just organisations. Future initiatives could explore lifecycle-based cyber literacy, from early childhood through to executive leadership, recognising that personal cyber behaviours directly affect organisational risk. Shared training models, particularly for small and not-for-profit operators, were identified as high-impact interventions.

AI AS A DEFENSIVE CAPABILITY

Rather than focusing solely on AI risk, participants highlighted the need to accelerate AI adoption for threat detection, anomaly monitoring, and operational assurance. Future roundtables could examine how agencies can safely deploy AI for defensive purposes, including behavioural analytics, deepfake detection, and adaptive authentication.

INNOVATIVE IDEAS AND CASE STUDIES

1. SECURE RESEARCH ENVIRONMENTS AS CAPABILITY MULTIPLIERS

The UTS Vault was highlighted as a practical example of how secure facilities can accelerate collaboration across government, industry, and academia. By providing accredited environments capable of handling protected and secret data, such facilities enable agencies to work on sensitive problems without duplicating infrastructure. Coupled with training and clearance sponsorship, these environments also address workforce shortages by building pipelines of security-cleared talent.

2. GRANULAR DATA PROTECTION AND TIME-BOUND ACCESS

Participants discussed emerging approaches to data security that move beyond perimeter controls. Concepts such as word-level encryption, attribute-based access, and time-bound decryption were presented as ways to align security with context. These approaches could support automated redaction for Freedom of Information requests, enforce deletion by design, and reduce reliance on manual controls.

3. CENTRALISED IDENTITY WITH CONTEXTUAL AUTHENTICATION

Several agencies described progress towards centralised identity ecosystems that support role-based access, step-up authentication for privileged users, and contextual verification. Examples included shifting from password complexity to password length, introducing adaptive multi-factor authentication, and exploring continuous authentication methods. These approaches aim to reduce friction while increasing assurance.

4. SHARED THREAT INTELLIGENCE NETWORKS

Information Sharing and Analysis Centres were identified as high-value mechanisms for collective defence. Participants described using shared channels to rapidly disseminate intelligence on emerging threats, reducing duplication and improving response times. However, concerns were raised about governance, record-keeping, and compliance when using encrypted messaging platforms, highlighting the need for clear organisational policies.

STRATEGIC OUTCOMES AND RECOMMENDATIONS

IMMEDIATE ACTIONS

- Conduct rapid audits of unstructured data to identify high-risk repositories and reduce unnecessary retention.
- Introduce contextual phishing simulations that focus on plausibility and behaviour, rather than technical cues.
- Implement warning-based controls for unauthorised AI tools, transitioning to blocking once awareness improves.
- Share prevention metrics with executive leadership to rebalance narratives away from failure-only reporting.

MEDIUM-TERM GOALS

- Establish centralised identity platforms that support adaptive authentication and reduce federated complexity.
- Embed data classification and labelling into everyday workflows, supported by automation.
- Expand access to low-cost or free cyber resilience training for small providers, non-profits, and community services.
- Formalise participation in threat intelligence sharing networks with clear governance and record-keeping frameworks.

LONG-TERM VISION

- Shift from perimeter-centric security models to data-centric and behaviour-aware architectures.
- Build cyber resilience into service design, ensuring continuity under attack or failure conditions.
- Develop workforce models that allow cyber teams to invest time in future threat planning, not just incident response.
- Foster a whole-of-society approach to cyber literacy, recognising that individual behaviours underpin system-wide resilience.

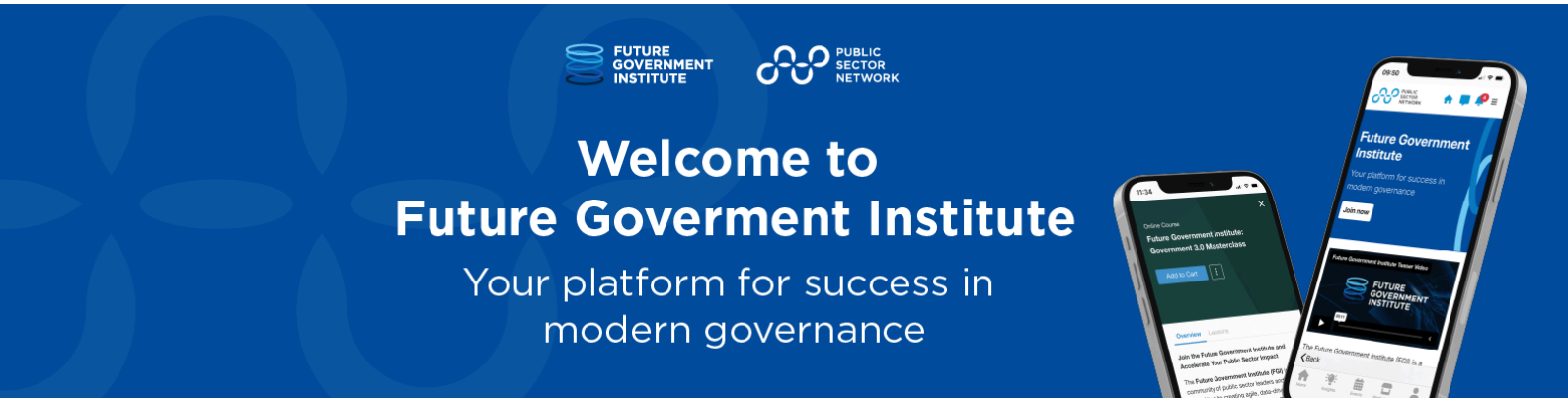
ABOUT THE FUTURE GOVERNMENT INSTITUTE (FGI) RESEARCH COUNCIL

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