

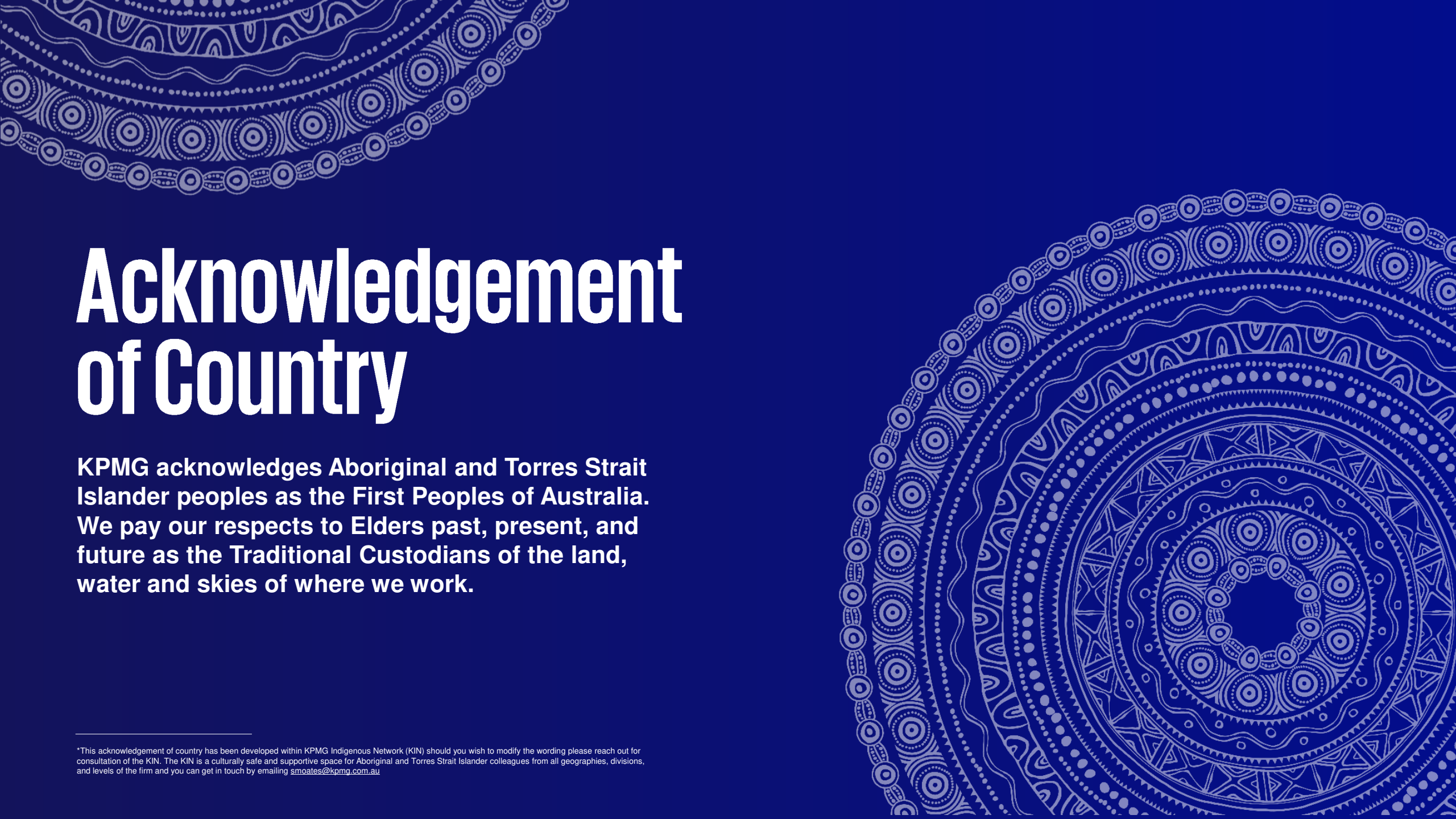


Cyber Security Research in Local Government Sector

Presentation for the Local Government
Technology Leadership Summit

March 2025





Acknowledgement of Country

KPMG acknowledges Aboriginal and Torres Strait Islander peoples as the First Peoples of Australia. We pay our respects to Elders past, present, and future as the Traditional Custodians of the land, water and skies of where we work.

*This acknowledgement of country has been developed within KPMG Indigenous Network (KIN) should you wish to modify the wording please reach out for consultation of the KIN. The KIN is a culturally safe and supportive space for Aboriginal and Torres Strait Islander colleagues from all geographies, divisions, and levels of the firm and you can get in touch by emailing smoates@kpmg.com.au

01

Introduction



©2025 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.

Document Classification: KPMG Confidential

Liability limited by a scheme approved under Professional Standards Legislation.

Meet Your Presenters



Liz Watts

Partner, National Local
Government Lead



Dominika Zerbe

Partner, Cyber Human Risk



©2025 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation. Document Classification: KPMG Confidential

Liability limited by a scheme approved under Professional Standards Legislation.

What will we cover today?

01

Why does Cyber Security in LG matter?

02

Overview of current Cyber Security Landscape

03

The four main challenges, their drivers and implications

04

What needs to change?

How big is the problem in Australia?



\$1m - 2m

Average total cost of a Council Data Breach

Factors that Amplify Cost



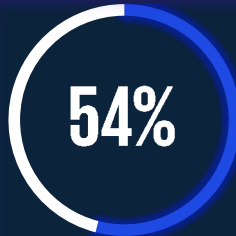
Security system complexity



Security skills shortage



Third-party breaches



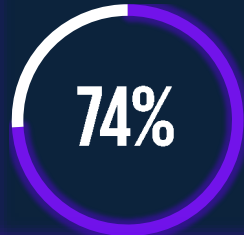
of all Australian companies were hit by a ransomware attack in 2024

Source: OneCloud IT Solutions



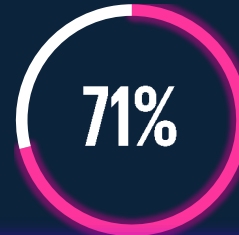
Of self reported cybercrimes were identity fraud

Source: ASD



of cyber breaches that were caused by the human element

Source: Infosec



Around 71% of extortion-related cyber security incidents involved ransomware

Source: ASD

Community Impact



Reputational damage



Confidential data loss



Critical service disruptions



Legal repercussions

02

Cyber Security in Local Government: Why it matters?



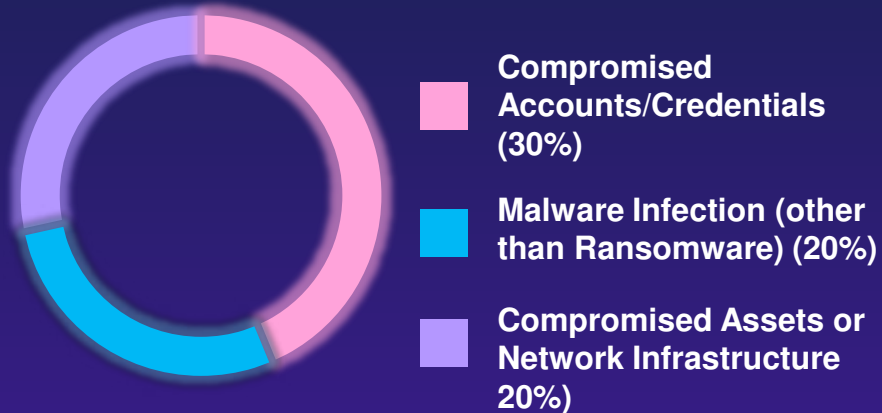
©2025 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.

Document Classification: KPMG Confidential

Liability limited by a scheme approved under Professional Standards Legislation.

Cyber Trends for Councils

Top 3 Cyber Incident Types Impacting Government



Source: ASD

88% of Victorian Local Councils in Western Australia experienced cyber security incidents in 2022 according to the Department of Security and Cybernetics

Source: Victorian Auditor General's Office

Published Cyber Attacks against or adjacent to councils

- Muswellbrook Shire Council || December 2024 || Ransomware Attack
- Unidentified || November 2024 || Programmable Logic Controllers (PLC)
- Goulburn Council || August 2023 || Compromised Facebook Account

In 2023, 50 councils in NSW had not implemented cyber security governance frameworks and relevant internal controls

Source: Audit Office of NSW

Councils are Facing Increases in the Frequency and Significance of Cyber Threats

1

Local Government stores many forms of sensitive data

2

Cyber attacks on Councils are increasing in occurrence and sophistication

3

There is limited guidance to protect Councils from Cyber Threats



94,000

Cybercrime reports were filed in Australia in FY23

Source: ASD

Threat Landscape

Ransomware Attacks

Phishing & Social Engineering Attacks

Supply Chain Attacks

Data Breaches & Privacy Violations

Artificially Enhanced Cybercrime

The Problem Statement Guiding the Research

?

What are the barriers and challenges that exist in cyber security in local governments?

?

What support is needed for the sector to systematically and holistically build and maintain its Cyber Security resilience?

01

The challenges



©2025 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.

Document Classification: KPMG Confidential

Liability limited by a scheme approved under Professional Standards Legislation.

Challenge 1: Fragmented and Inconsistent Standards and Frameworks

Overview and Current Landscape:

- Councils in Australia face challenges in cyber security due to varying state and federal regulations.
- Cyber requirements differ by services and jurisdictions, adding complexity.
- Lack of a unified national framework leads to inconsistent cyber risk management across local governments.

Drivers

-  **Resource Disparities**
-  **Lack of Federal Coordination**
-  **State Autonomy**

Implications

-  **Compliance Gaps and Security Vulnerabilities**
-  **Administrative Burden**
-  **Reduced Transparency and Accountability**

Challenge 2: Budgetary Constraints and Resource Limitations

Overview and Current Landscape:

- Councils in Australia prioritise digital transformation and physical infrastructure over cyber security, creating vulnerabilities.
- Physical projects get more funding due to immediate benefits and legislative requirements.
- Cyber security is discretionary and often undervalued compared to tangible projects.

Drivers

-  **Competing Priorities**
-  **Low Perceived Value Internally and Externally**
-  **Reactive Funding Approach**

Implications

-  **Increased Vulnerability**
-  **Delayed Incident Response and Recovery**
-  **Reactive Rather than Proactive Security**

Challenge 3: Shortage of Cyber Security Expertise and Capacity

Overview and Current Landscape:

- Councils in Australia struggle with cyber security due to a shortage of expertise and capacity.
- Limited budgets hinder Councils' ability to attract top cyber security professionals.
- Rural and remote Councils are particularly affected by the nationwide talent shortage.

Drivers

-  **Limited budgets and Resource Constraints**
-  **Insufficient Training and Education**
-  **High Demand and Competition for Talent**

Implications

-  **Increased Vulnerability**
-  **Inadequate Response Capabilities**
-  **Diminished Cyber Security Culture**

Challenge 4: Low Adoption of Controls and Risk Management practices

Overview and Current Landscape:

- Councils in Australia struggle to manage cyber security risks due to low adoption of essential controls.
- Implementing frameworks like the Essential 8 is resource-intensive and needs specialised expertise.
- Both outdated IT systems and new digital services can increase cyber security risks if not properly protected.

Drivers

-  **Budget and Resource Limitations**
-  **Complexity of Standards or Frameworks**
-  **Technological Changes**
-  **Limited Support from Federal Government**

Implications

-  **Increased Cyber Security Risk**
-  **Potential Disruptions to Services**
-  **Higher Long-Term Costs**
-  **Vulnerability in Digital Transformation**

01

Solutions



©2025 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.

Document Classification: KPMG Confidential

Liability limited by a scheme approved under Professional Standards Legislation.

The recommendations for strengthening cyber security in Local Government are focused on the themes of policy, resources, education and support



Establish consistent policies nation-wide

What does this look like?

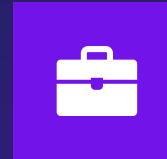
Standardise cyber practices across Councils nationally to enhance Council performance and strengthen national security



Resolve resourcing and funding issues

What does this look like?

Ensure funding and resources are efficiently allocated and utilised for enhancing cyber security in Councils



Uplift education and awareness

What does this look like?

Clarify the gaps in cyber security culture (knowledge, behaviour, attitude) & develop targeted education & training for Councils



Partner together for consistent support

What does this look like?

Enhance the support systems for Council cyber security to ensure consistent guidance and resources are delivered



Contact Us



Liz Watts
Partner, National Local Government
Sector Lead

T: +61 416 081 608

E: ewatts@kpmg.com.au



Dominika Zerbe - Anders
Partner, Cyber Human Risk & Resilience

T: +61 7 3233 9504

E: dzerbe@kpmg.com.au

Read our Thought Leadership



[Cyber security considerations 2024](#)



[Cyber security in Local Government](#)



[Unlocking capabilities to uplift service experience](#)