- **3 Information and Cyber Security Policy**

--ooOOoo--

Item 3 / Minutes Attachment 1

Purpose

- To provide The Mayor and Councilor's with an overview of Ipswich City Council’s current cyber security environment, including key risks, our work to protect ICC and future priorities.
- To outline how Council is aligning to its Information and Cyber Security Policy to safeguard community data, services, and trust.

2

ICC Cyber Risk Profile

Rising Cybercrime Frequency

Cybercrime incidents in Australia **occur every seven minutes**, highlighting a rapidly escalating threat landscape.

Targeted Government Agencies

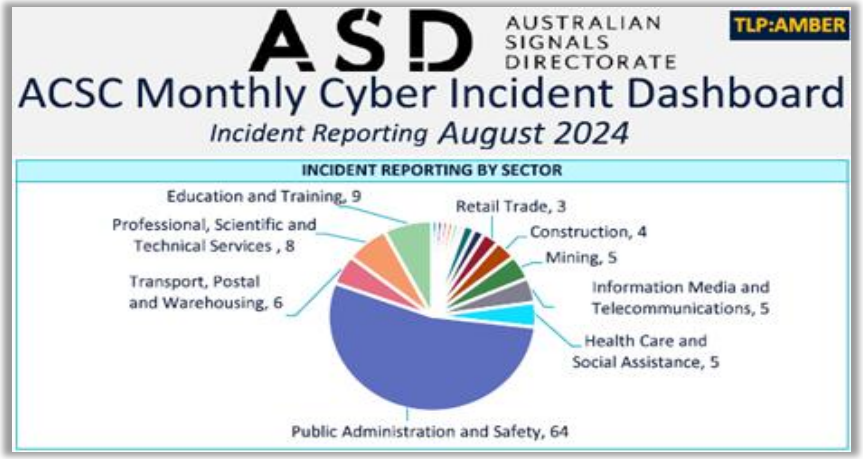
Local councils are prime targets due to access to personal data and critical infrastructure.

Financial and Operational Impact

Cyber incidents could potentially cost Ipswich City Council millions in losses and reputational damage.

Key Threat Vectors

Phishing, malware, ransomware, and third-party vulnerabilities are primary attack methods requiring vigilance.



ICC Cyber Maturity

The Essential Eight Maturity Model, developed by the Australian Cyber Security Centre, sets out eight practical strategies to strengthen an organisation's cyber resilience. Ipswich City Council is progressing strongly against this model and is very close to achieving Level 2, reflecting a significant uplift in our defences.

ICC Cyber Current State

Cyber Security Roadmap Achievements

Eliminated end-of-life infrastructure to reduce residual cybersecurity risks.

Essential 8 Uplift Project

Progress toward Essential 8 Level 2 compliance - currently at 85%, with significant advancements across all eight security pillars.

Phriendly Phishing Platform

Implemented streamlined phishing reporting, monthly targeted training and onboarding program to build a culture of security awareness and shared responsibility.

Improved Cyber Maturity Score

Increased cyber maturity from 74% to 82%, enhancing identity, data, and device security.

ICC Cyber Future State

Cybersecurity Strategy

Six pillars guide secure tech use, data protection, incident response, staff engagement, supply chain risk, and compliance & risk reporting.

Continuing Maturity

Strategic goals includes enhancing operational capabilities, conducting simulations, and periodic penetration testing and process improvements.

Workforce and Vendor Management

Fostering a security-aware workforce and maintaining strict oversight of third-party vendors ensures robust protection.

Compliance and Framework Alignment

The vision aligns with Essential 8 and where practicable ISO27001 standards, ensuring comprehensive compliance and transparent reporting.

Strategy Pillars

01

Leverage

Emerging Technologies Securely

Enable Council to safely adopt and integrate emerging technologies such as AI, cloud and SaaS solutions through the assessment and selection of secure technologies.

02

Protect

Council Information & Systems

Safeguard sensitive information, services, and critical infrastructure against cyber-attacks through effective vulnerability management.

03

Strengthen

Incident Response & Resilience

Improve Council's ability to detect, respond to, and recover from cyber incidents using intelligence sharing, SOC operations, tabletop and simulated exercises.

04

Engage

By Promoting a Security-Aware Workforce

Create a culture of security awareness through continuous education, training, phishing testing, simulation, and compliance programs.

05

Manage

3rd Party Supply Chain

Effectively manage cyber risks associated with 3rd party supply chains by working with vendors to provide assurance and oversight.

06

Govern

Compliance, Risk & Reporting

Maintain adherence to legal, regulatory, and compliance requirements by aligning with best practice essential 8 and ISO27001 standards.

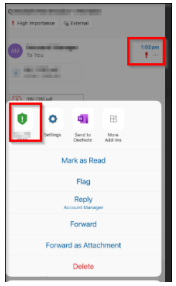
Summary and next steps

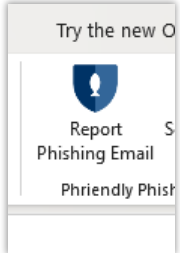
Summary

- Cyber incidents are increasing in frequency and targeting local government.
- Council has uplifted its cyber resilience, improving its maturity score from **74% to 82%** and progressing strongly towards **Essential Eight Level 2**.
- Key initiatives delivered include the **Cyber Roadmap achievements**, **Essential Eight uplift**, and the **Phriendly Phishing awareness platform**.
- Council now ranks in the **top 10 secure scores across Queensland government agencies**.

Next Steps

- Stay vigilant, if you notice a suspicious email report immediately by clicking these buttons in Outlook.





7

Questions/Discussion

8